



AVG 9 Anti-Virus

Kullanıcı Kılavuzu

Belge revizyonu 90.21 (3.2.2010)

Telif Hakkı AVG Technologies CZ, s.r.o. Tüm hakları saklıdır.
Tüm diğer ticari markalar, ilgili sahiplerine aittir.

Bu ürün, RSA Data Security, Inc. MD5 Message-Digest Algorithm özelliğini kullanmaktadır, Telif Hakkı (C) 1991-2, RSA Data Security, Inc. Oluşturma Tarihi: 1991.

Bu üründe, C-SaCzech kütüphanesi, Telif Hakkı (c) 1996-2001 Jaromir Dolecek (dolecek@ics.muni.cz) kodları kullanılmaktadır.

Bu ürün sıkıştırma kitaplığı zlib ürününü kullanmaktadır, Telif Hakkı (c) 1995-2002 Jean-loup Gailly ve Mark Adler.

Bu ürün sıkıştırma kitaplığı libbzip2 kullanır, Telif Hakkı (c) 1996-2002 Julian R. Seward.

İçindekiler

1. Giriş	7
2. AVG Yükleme Gereksinimleri	8
2.1 Desteklenen İşletim Sistemleri	8
2.2 Minimum ve Önerilen Donanım Gereksinimleri	8
3. AVG Yükleme Seçenekleri	9
4. AVG Download Manager	10
4.1 Dil Seçimi	10
4.2 Bağlantı Sınama	11
4.3 Proxy Ayarları	12
4.4 Yüklenecek Dosyaları İndirin	13
5. AVG Yükleme Süreci	14
5.1 Yükleme Başlatma	14
5.2 Lisans Sözleşmesi	15
5.3 Sistem Durumu Kontrolü	15
5.4 Yükleme Türü Seçin	16
5.5 AVG Lisansınızı Etkinleştirin	16
5.6 Özel Yükleme - Hedef Klasör	17
5.7 Özel Yükleme - Bileşen Seçimi	18
5.8 AVG DataCenter	19
5.9 AVG Security Toolbar	20
5.10 Açık uygulamaları kapatın	21
5.11 AVG Yükleniyor	22
5.12 Düzenli tarama ve güncellemeleri programlamak	23
5.13 AVG koruması yapılandırması tamamlandı	23
6. Yüklemeden Sonra	25
6.1 Taramayı en iyi hale getirme	25
6.2 Ürün Kaydı	25
6.3 Kullanıcı Arayüzü'ne Eriş	25
6.4 Tam bilgisayar taraması	26
6.5 Eicar Testi	26
6.6 AVG Varsayılan Yapılandırması	27

7. AVG Kullanıcı Arayüzü	28
7.1 Sistem Menüsü	29
7.1.1 Dosya	29
7.1.2 Bileşenler	29
7.1.3 Geçmiş	29
7.1.4 Araçlar	29
7.1.5 Yardım	29
7.2 Güvenlik Durumu Bilgisi	32
7.3 Hızlı Bağlantılar	33
7.4 Bileşen Genel Görünümü	33
7.5 İstatistikler	34
7.6 Sistem Tepsisi Sembolü	35
8. AVG Bileşenleri	36
8.1 Virüsten Koruma	36
8.1.1 Virüsten Koruma İlkeleri	36
8.1.2 Virüsten Koruma Arayüzü	36
8.2 Casus Yazılımdan Koruma	38
8.2.1 Casus Yazılımdan Koruma Prensipleri	38
8.2.2 Casus Yazılımdan Koruma Arayüzü	38
8.3 Rootkit Önleme	40
8.4 E-Posta Tarayıcısı	40
8.4.1 E-posta Tarayıcısı Prensipleri	40
8.4.2 E-posta Tarayıcısı Arayüzü	40
8.4.3 E-posta Tarayıcısı Tespiti	40
8.5 Lisans	44
8.6 Bağlantı Tarayıcı	45
8.6.1 Link Scanner Prensipleri	45
8.6.2 Link Scanner Arayüzü	45
8.6.3 AVG Arama Kalkanı	45
8.6.4 AVG Aktif Gezinme Kalkanı	45
8.7 Çevrimiçi Kalkan	49
8.7.1 Online Shield İlkeleri	49
8.7.2 Online Shield Arayüzü	49
8.7.3 Online Shield Algılaması	49
8.8 Yerleşik Kalkan	55
8.8.1 Yerleşik Kalkan Prensipleri	55

8.8.2 Yerleşik Kalkan Arayüzü	55
8.8.3 Yerleşik Kalkan Tespiti	55
8.9 Güncelleme Yöneticisi	60
8.9.1 Güncelleme Yöneticisi Prensipleri	60
8.9.2 Güncelleme Yöneticisi Arayüzü	60
9. AVG Security Toolbar	63
9.1 AVG Security Toolbar Arayüz	63
9.2 AVG Security Toolbar Seçenekleri	65
9.2.1 Genel Sekmesi	65
9.2.2 Yararlı Düğmeler Sekmesi	65
9.2.3 Güvenlik Sekmesi	65
9.2.4 Gelişmiş Seçenekler Sekmesi	65
10. AVG Gelişmiş Ayarlar	70
10.1 Görünüm	70
10.2 Sesler	72
10.3 Hatalı Durumları Yoksay	74
10.4 Virüs Kasası	75
10.5 PUP İstisnaları	76
10.6 Çevrimiçi Kalkan	79
10.6.1 Web Koruması	79
10.6.2 Anlık Mesajlaşma	79
10.7 Bağlantı Tarayıcı	83
10.8 Taramalar	84
10.8.1 Tüm Bilgisayarı Tara	84
10.8.2 Kabuk Uzantısı Tarama	84
10.8.3 Belirli Dosyaları veya Klasörleri Tara	84
10.8.4 Çıkarılabilir Aygıt Tarama	84
10.9 Programlar	91
10.9.1 Programlı Tarama	91
10.9.2 Virüs Veritabanı Güncelleme Programı	91
10.10 E-Posta Tarayıcısı	102
10.10.1 Sertifikasyon	102
10.10.2 Posta Filtreleme	102
10.10.3 Günlükler ve Sonuçlar	102
10.10.4 Sunucular	102
10.11 Yerleşik Kalkan	112

10.11.1 Gelişmiş Ayarlar	112
10.11.2 Hariç Tutulan Dizin	112
10.11.3 Hariç Tutulan Dosyalar	112
10.12 Önbellemek Sunucusu	117
10.13 Rootkit Önleme	118
10.14 Güncelle	120
10.14.1 Proxy	120
10.14.2 Çevirmeli	120
10.14.3 URL	120
10.14.4 Yönet	120
10.15 Uzaktan Yönetim	127
11. AVG Tarama	129
11.1 Tarama Arayüzü	129
11.2 Öntanımlı Taramalar	130
11.2.1 Tüm Bilgisayarı Tara	130
11.2.2 Belirli Dosyaları veya Klasörleri Tara	130
11.3 Windows Gezgininde Tarama	138
11.4 Komut Satırı Tarama	139
11.4.1 CMD Tarama Parametreleri	139
11.5 Tarama Planlama	142
11.5.1 Program Ayarları	142
11.5.2 Tarama Şekli	142
11.5.3 Taranacaklar	142
11.6 Tarama Sonuçları Genel Görünümü	152
11.7 Tarama Sonuçları Ayrıntılar	153
11.7.1 Sonuçlara Genel Bakış Sekmesi	153
11.7.2 Bulaşma Sekmesi	153
11.7.3 Casus Yazılım Sekmesi	153
11.7.4 Uyarılar Sekmesi	153
11.7.5 Kök Kullanıcı Sekmesi	153
11.7.6 Bilgi Sekmesi	153
11.8 Virüs Kasası	162
12. AVG Güncellemeleri	164
12.1 Güncelleme Seviyeleri	164
12.2 Güncelleme Türleri	164
12.3 Güncelleme İşlemi	165



13. Olay Geçmişi	166
14. SSS ve Teknik Destek	168



1. Giriş

Bu kullanıcı el kitabı, **AVG 9 Anti-Virus** için kapsamlı dokümantasyon sağlar.

AVG 9 Anti-Virus programını satın aldığınız için tebrik ederiz!

AVG 9 Anti-Virus PC'niz için tam güvenlik ve rahatlık sağlamak üzere tasarlanmış ödüllü AVG ürünlerinden biridir. AVG'nin ünlü ve ödüllü güvenlik korumasını sunmak adına bastan basa tamamen yeniden tasarlanan **AVG 9 Anti-Virus**, tüm diğer AVG ürünleri gibidir fakat kullanımı daha kolay ve verimlidir.

Yeni **AVG 9 Anti-Virus** ürününüz daha agresif ve daha hızlı taramayı birleştiren akıcı bir arayüze sahiptir. Güvenliğiniz için daha fazla sayıda güvenlik özelliği otomatik hale getirilmiştir ve yeni 'akilli' kullanıcı seçenekleri sayesinde gerekli ayarlamaları kendi güvenlik ihtiyaçlarınız doğrultusunda yapabilirsiniz. Artık güvenliğinizden ödün vermek yok!

AVG, bilisim ve ağ kurma faaliyetlerinizi korumak için tasarlanmış ve geliştirilmiştir. AVG'nin sağladığı eksiksiz korumanın tadını çıkartın.



2. AVG Yükleme Gereksinimleri

2.1. Desteklenen İşletim Sistemleri

AVG 9 Anti-Virus aşağıdaki işletim sistemlerine sahip iş istasyonlarını koruma amaçlıdır:

- Windows 2000 Professional SP4 + Güncelleme Paketi 1
- Windows XP Home Edition SP2
- Windows XP Professional SP2
- Windows XP Professional x64 Edition SP1
- Windows Vista (x86 ve x64, tüm sürümleri)
- Windows 7 (x86 ve x64, tüm sürümler)

(ve belirli işletim sistemleri için daha yeni servis paketleri)

2.2. Minimum ve Önerilen Donanım Gereksinimleri

AVG 9 Anti-Virus için minimum donanım gereksinimleri:

- Intel Pentium CPU 1,5 GHz
- 512 MB RAM bellek
- 390 MB boş sabit disk alanı (yükleme için)

AVG 9 Anti-Virus için önerilen donanım gereksinimleri:

- Intel Pentium CPU 1,8 GHz
- 512 MB RAM bellek
- 510 MB boş sabit disk alanı (yükleme için)



3. AVG Yükleme Seçenekleri

AVG, yükleme CD'niz üzerinde bulunan yükleme dosyasından yüklenebilir ya da en güncel yükleme dosyasını AVG'nin web sitesinden (<http://www.avg.com/>) indirebilirsiniz.

AVG'yi yüklemeye başlamadan önce yeni yükleme dosyasını kontrol etmek için AVG web sitesini (<http://www.avg.com/>) ziyaret etmenizi önemle öneririz. Bu şekilde, en güncel AVG 9 Anti-Virus sürümünü yüklediğinizden emin olabilirsiniz.

Yükleme dosyasını gerekli dilde ayarlamanıza yardımcı olacak yeni [AVG Download Manager](#) aracımızı denemenizi öneririz!

Yükleme işlemi sırasında lisans/satis numaranızı girmeniz istenecektir. Yüklemeye başlamadan önce söz konusu numarayı hazırladığınızdan emin olun. Satis numarası, CD ambalajı üzerinde bulunur. AVG'yi çevrimiçi mağazadan satın aldıysanız lisans numaranız e-posta aracılığıyla gönderilecektir.

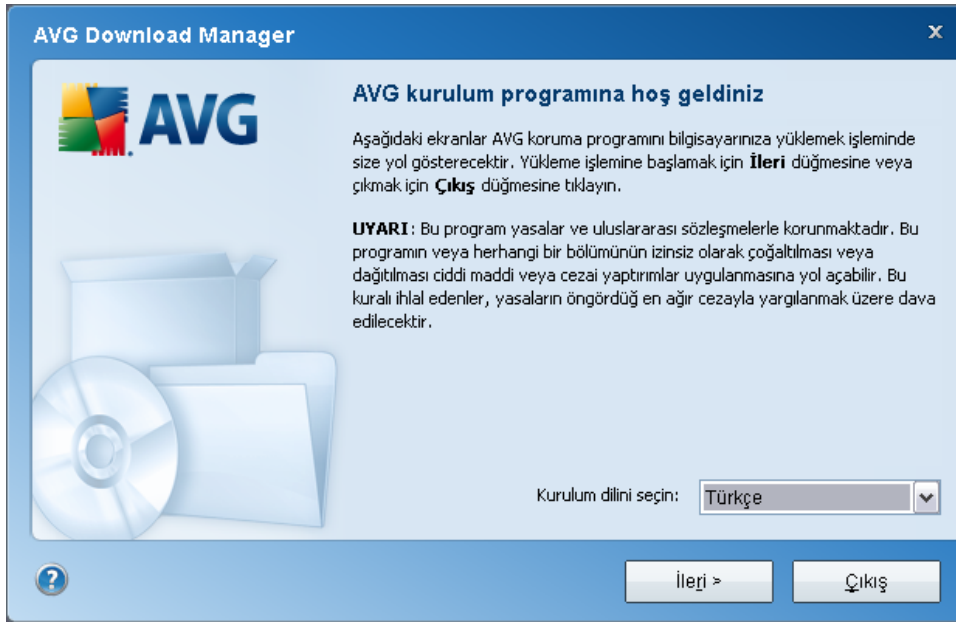
4. AVG Download Manager

AVG Download Manager, AVG ürününüzün deneme sürümü için uygun yükleme dosyasını seçmenize yardımcı olan basit bir araçtır. Girdiğiniz bilgilere dayanarak yönetici, belirli bir ürünü, lisans türü, istenen bileşenleri ve dili seçecektir. Son olarak, **AVG Download Manager** karsıdan yüklemeye devam edecek ve uygun [yükleme işlemini](#) başlatacaktır.

Uyarı: AVG Download Manager ag ve SBS sürümlerini indirmeye uygun değildir ve yalnızca aşağıdaki işletim sistemleri desteklenir: Windows 2000 (SP4 + SRP toplu), Windows XP, Windows Vista, Windows 7.

AVG Download Manager, AVG web sitesinden (<http://www.avg.com/>) indirilebilir. Aşağıda **AVG_DOWNLOAD_MANAGER%** kapsamında izlemeniz gereken adımlar kısaca açıklanmıştır:

4.1. Dil Seçimi

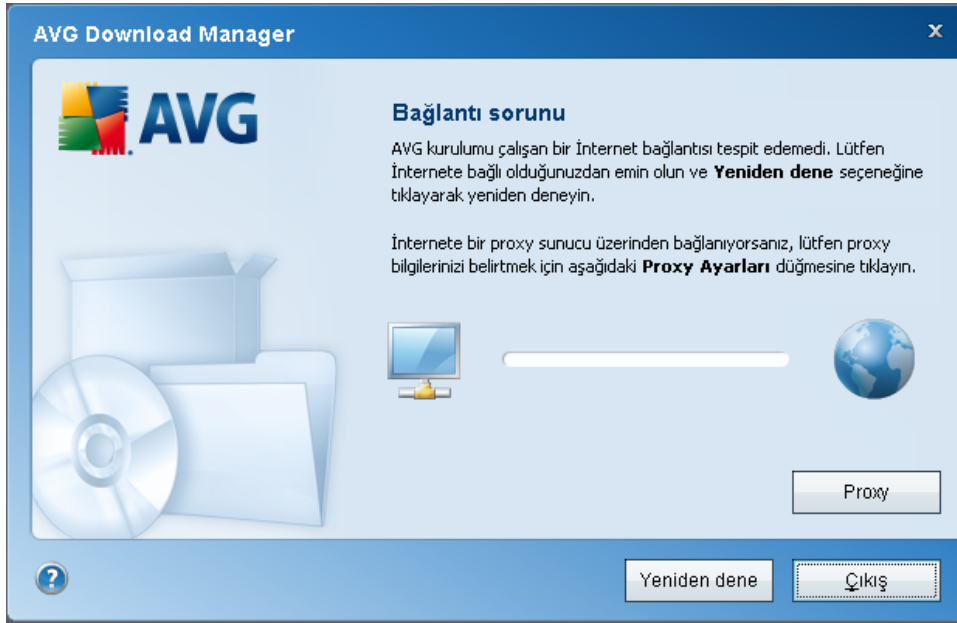


AVG Download Manager ilk adımında açılır menüden yükleme dilini seçin. Dil seçiminizin sadece yükleme işlemine ilişkin olduğunu ve yüklemenin hemen ardından dili program ayarlarından değiştirebileceğinizi unutmayın. Ardından devam etmek için **İleri** düğmesine basın.

4.2. Bağlantı Sınama

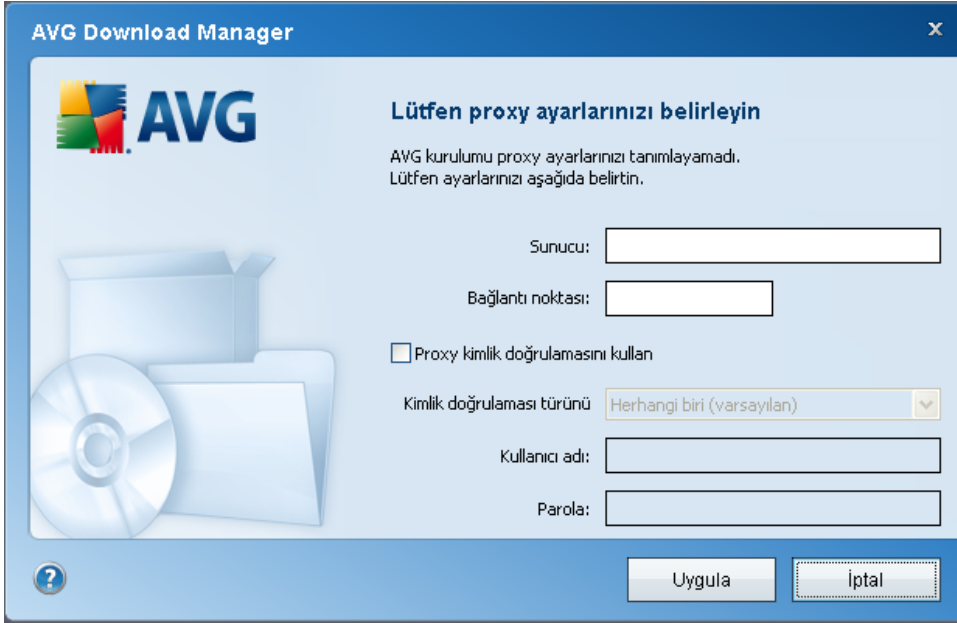
Bu adımda, **AVG Download Manager**, bir İnternet bağlantısı kurmaya çalışacak, bu yüzden güncellemeler bulunabilir. **AVG Download Manager**, indirme yöneticisi bağlantı testini tamamlayana kadar indirme işlemine geçmenize izin verilmeyecektir.

- Testin sonucunda herhangi bir bağlantı bulunamazsa İnternet'e bağlı olduğunuzdan emin olun. Ardından **Yeniden Dene** düğmesine tıklayın.



- İnternet'e Proxy bağlantısı ile bağlanıyorsanız **Proxy Ayarları** düğmesine tıklayıp [proxy bilgilerinizi](#) tanımlayın:
- Test başarılı sonuçlanırsa devam etmek için **İleri** düğmesine basın.

4.3. Proxy Ayarları

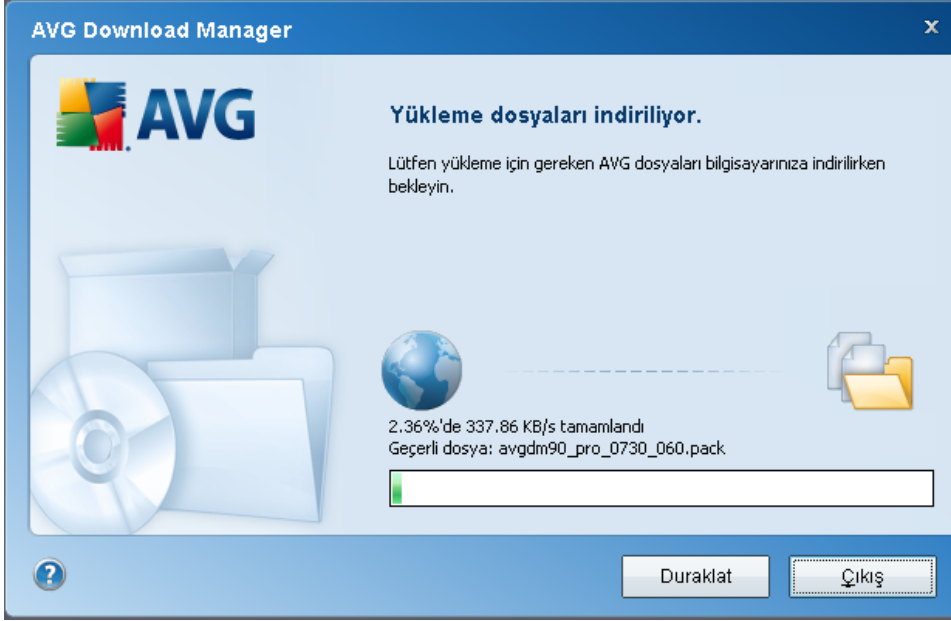


AVG Download Manager, Proxy ayarlarınızı tanımlayamıyorsa manüel olarak girmelisiniz. Lütfen aşağıdaki bilgileri doldurun:

- **Sunucu** - geçerli bir proxy sunucu adı ya da IP adresi girin
- **Bağlantı Noktası** - ilgili bağlantı noktası numarasını girin
- **Proxy kimlik doğrulamayı kullan** - Proxy sunucunuzun kimlik doğrulama gerektirmesini istiyorsanız bu kutuyu işaretleyin.
- **Kimlik doğrulama seç** - açılır menüden kimlik doğrulama türünü seçin. Öntanımlı değerleri değiştirmemenizi önemle tavsiye ediyoruz (*ardından proxy sunucusu gereksinimlerinin otomatik olarak sizin tarafınızdan karşılanmasını bekleyecektir*). Diğer bir yandan deneyimli bir kullanıcıysanız Temel (*bazı sunucular tarafından talep edilir*) ya da NTLM (*ISA Sunucuları tarafından talep edilir*) seçeneklerinden birini seçebilirsiniz. Ardından geçerli bir **Kullanıcı Adı** ve **Parolası** girin (isteğe bağlı).

AVG Download Manager ögesinin bir sonraki aşamasına geçebilmek üzere **Uygula** düğmesine basarak ayarlarınızı onaylayın.

4.4. Yüklenecek Dosyaları İndirin



Artık, **AVG Download Manager** programının yükleme paketini indirmesi ve yükleme sürecini başlatması için tüm bilgileri sağladınız. Daha sonra, [AVG Yükleme Süreci](#)'ne geçin.

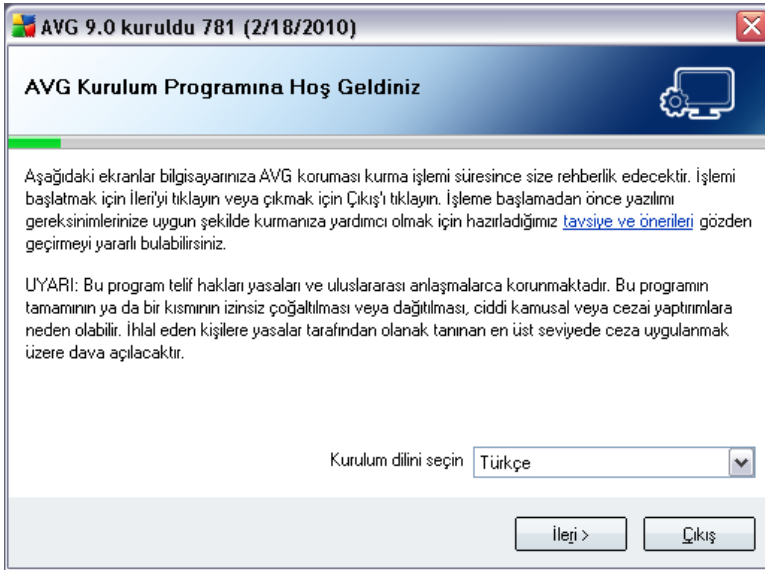


5. AVG Yükleme Süreci

Bilgisayarınıza **AVG 9 Anti-Virus** programını yüklemek için, en güncel yükleme dosyasını edinmeniz gerekir. Kutulu versiyonların içinden çıkan CD'de bulunan yükleme dosyasını da kullanabilirsiniz fakat söz konusu dosya güncel olmayabilir. Bu nedenle en güncel kurulum dosyasını çevrimiçi ortamdan indirmenizi öneriyoruz. Dosyayı AVG web sitesinden (<http://www.avg.com/>), **Destek Merkezi / Indir** kısmından indirebilirsiniz. Ya da ihtiyacınız olan kurulum paketini oluşturmaya ve indirmeye ve yükleme işlemini başlatmaya yardımcı olacak yeni **AVG Download Manager** aracımızı da kullanabilirsiniz.

Yükleme işlemi, her adımda neler yapmanız gerektiğine dair kısa tanımlamalar içeren bir dizi iletişim kutusu pencerelerinden oluşur. Aşağıda iletişim kutularının her biri için kısa bir açıklama sunuyoruz:

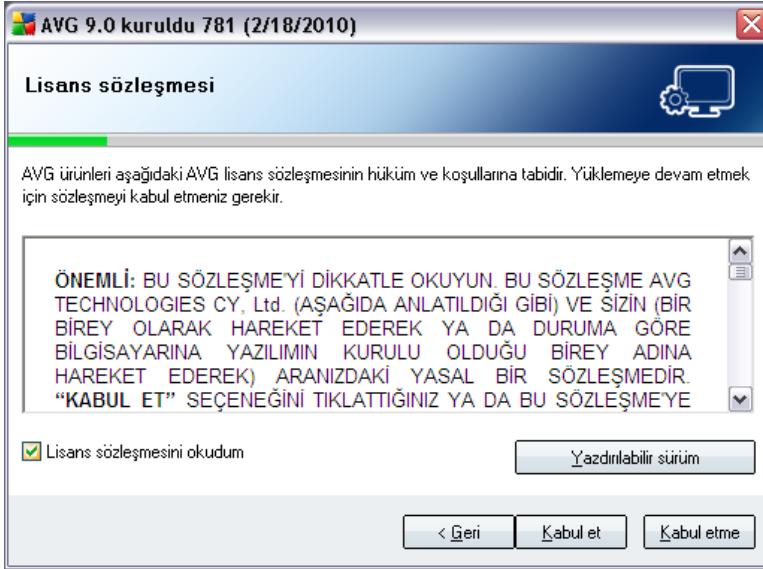
5.1. Yükleme Başlatma



Yükleme işlemi, **AVG Yükleme Programına Hoş Geldiniz** penceresi ile başlar. Burada yükleme işlemi için kullanacağınız dili seçebilirsiniz. İletişim kutusu penceresinin alt kısmında **Kurulum dilinizi seçin** ögesini bulun ve açılır menüden istediğiniz dili seçin. Onaylamak ve bir sonraki iletişim kutusuna geçmek için **İleri** düğmesine basın.

Dikkat: Burada sadece yükleme işlemi sırasında kullanılacak dili seçersiniz. AVG yükleme işleminin son aşamalarında seçilmesi gereken AVG uygulamasına ilişkin dil bu pencerede seçilmez.

5.2. Lisans Sözleşmesi



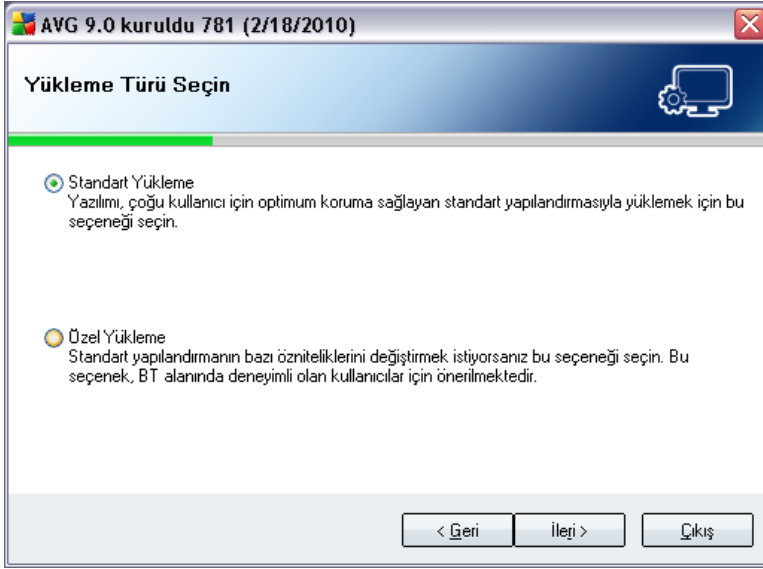
Lisans Sözleşmesi iletişim kutusunda AVG lisans sözleşmesinin tamamı bulunmaktadır. Lütfen sözleşmeyi dikkatle okuyun ve **Lisans sözleşmesini okudum** onay kutusunu işaretleyerek ve **Kabul ediyorum** düğmesine basarak okudugunuzu, anladığınızı ve kabul ettiğinizi onaylayın.

Lisans sözleşmesini kabul etmiyorsanız **Kabul Etmiyorum** düğmesine basın; yükleme işlemi anında iptal edilecektir.

5.3. Sistem Durumu Kontrolü

Lisans sözleşmesini onayladıktan sonra **Sistem Durumu Kontrol Ediliyor** iletişim kutusuna yönlendirileceksiniz. Bu iletişim kutusu herhangi bir müdahale gerektirmez; AVG yüklemesi başlamadan önce sisteminiz kontrol edilir. Lütfen işlem bitene kadar bekleyin ve ardından bir sonraki iletişim kutusuna otomatik olarak geçin.

5.4. Yükleme Türü Seçin



Yükleme Tipini Seç iletişim kutusunda iki farklı yükleme seçeneği sunulur: **standart** ve **özel** kurulum.

Kullanıcıların çoğu için yazılım geliştiricisi tarafından öntanımlı ayarlarla AVG'yi tamamen fonksiyonel şekilde kuran **standart kurulum** önerilmektedir. Bu yapılandırma, minimum kaynak kullanımı ile maksimum güvenliği bir araya getirir. Gelecekte söz konusu yapılandırmayı değiştirme ihtiyacı duyarsanız söz konusu işlemi doğrudan AVG uygulamasından yapabileceksiniz.

Özel yükleme AVG'yi standart olmayan ayarlarla kurmak hususunda geçerli bir nedeni olan deneyimli kullanıcılar tarafından kullanılmalıdır. Örn. belirli sistem gereksinimlerini karşılamak için.

5.5. AVG Lisansınızı Etkinleştirin

AVG Lisansınızı Etkinleştirin iletişim kutusunda kayıt bilgilerinizi girmeniz gerekir. Adınızı (**Kullanıcı Adı** alanına) ve organizasyon adınızı (**Sirket Adı** alanına) girin.

Lisans/satis numaranızı **Lisans Numarası** alanına girin. Satis numarası, **AVG 9 Anti-Virus** kutusundaki CD paketinde bulunabilir. Lisans numarası **AVG 9 Anti-Virus** programını çevrimiçi satın aldıktan sonra alacağınız onay e-postasında olacaktır. Sayıları gösterildiği gibi gitmelisiniz. Lisans numarasının dijital formu mevcut ise (**e-postada**) girmek için kopyala ve yapıştır yönteminin kullanılması önerilmektedir.

AVG 9.0 kuruldu 781 (2/18/2010)

AVG Lisansınızı etkinleştirin

Kullanıcı adı:

Şirket adı:

Lisans numarası:

Örnek: 9FULL-NSDRS-KUL4L-UKSFR-L96M9-B2<-XWMMX

Yazılımı çevrimiçi satın aldıysanız, lisans numaranız e-posta ile gönderilecektir. Yazım hatalarını önlemek için numarayla e-postanızdan kopyalayıp bu ekrana yapıştırmanızı öneririz.

Yazılımı bir mağazadan satın aldıysanız, lisans numarasını paketin içindeki ürün kayıt kartı üzerinde bulabilirsiniz. Numarayla doğru şekilde kopyalamaya dikkat edin.

< Geri İleri > Çıkış

Yükleme işlemine devam etmek için **İleri** düğmesine basın.

Bir önceki asamada standart yüklemeyi seçtiyseniz doğrudan **AVG Security Toolbar iletişim kutusuna yönlendirileceksiniz**. Özel kurulumu seçtiyseniz **Hedef Klasör** iletişim kutusu ile devam edeceksiniz.

5.6. Özel Yüklemeye - Hedef Klasör

AVG 9.0 kuruldu 781 (2/18/2010)

Hedef Klasör

Varsayılan hedef klasör aşağıda gösterilmektedir. Farklı bir klasör seçmek için Göz at düğmesine tıklayabilirsiniz ancak biz varsayılan ayarları kullanmanızı öneririz.

Hedef klasör:

Göz at

< Geri İleri > Çıkış

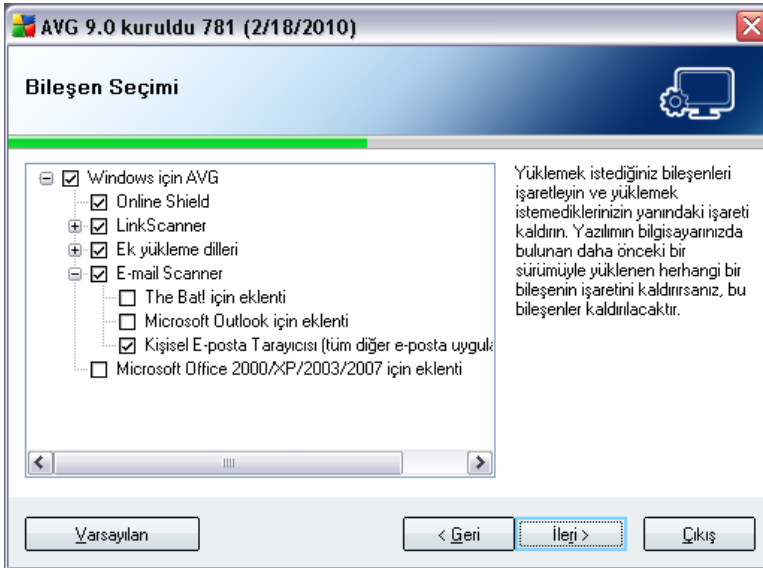


Hedef Klasör iletisim kutusu, **AVG 9 Anti-Virus** programinin yüklenmesi gereken yeri belirtmenizi sağlar. Varsayılan olarak AVG, C: Sürücüsü üzerinde program dosyaları klasörüne yüklenecektir. Klasör henüz yoksa, yeni bir iletisim kutusunda AVG'nin bu klasörü şimdi olusturmasını kabul etmeniz istenecektir.

Bu konumu degistirmek istiyorsanız, sürücü yapısını görüntülemek ve ilgili klasörü seçmek için **Gözet** düğmesini kullanın.

Onaylamak için **İleri** düğmesini tıklatin.

5.7. Özel Yükleme - Bileşen Seçimi



Bilesen Seçimi iletisim kutusu, yüklenebilir **AVG 9 Anti-Virus** bilesenlerine genel bir bakış görüntüler. Varsayılan ayarların size uygun olmaması halinde belirli bilesenleri kaldırabilir ya da ekleyebilirsiniz.

Diger bir yandan sadece satın aldığınız AVG sürümü kapsamında bulunan bilesenler arasında seçim yapabilirsiniz. Bilesen Seçimi iletisim kutusunda yüklenmesi için sadece söz konusu bilesenler sunulur.

• Dil seçimi

Yüklenecek bilesenler listesinde AVG ile birlikte yüklenecek dili (dilleri) seçebilirsiniz. **Ekstra yüklenen diller** ögesini işaretleyin ve sonra ilgili menüden istediğiniz dilleri seçin.

- **E-Posta Tarayicisi eklentileri**

Elektronik postalarinizin güvenliğini sağlamak üzere yüklenecek eklentiler hususunda karar vermek ve açmak için **E-Posta Tarayicisi** ögesini tıklayın. Varsayılan olarak **Microsoft Outlook Eklentisi** yüklenecektir. Diğer bir seçenek ise **The Bat! eklentisidir**. Baska bir e-posta istemcisi kullanıyorsanız (MS Exchange, Qualcomm Eudora...), **Kişisel E-Posta Tarayicisi** seçeneğine gidin ve kullandığınız e-posta programının ne olduğu önemli olmaksızın e-posta görüşmelerinizi otomatik olarak güven altına alın.

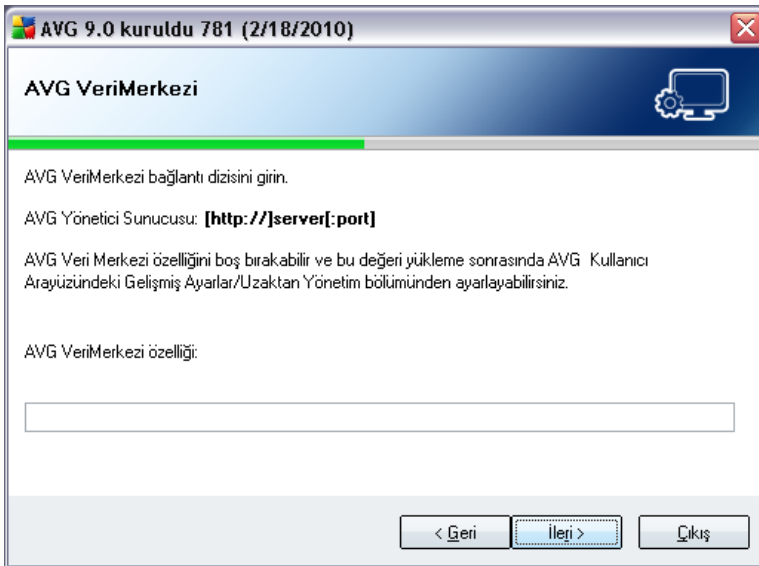
- **Uzaktan Yönetim**

Bilgisayarınızı AVG Remote Administration'a daha sonra bağlamak istiyorsanız, lütfen yüklenecek ilgili ögeyi de işaretleyin.

İleri düğmesine basarak devam edin.

5.8. AVG DataCenter

AVG ag lisansı kullanılıyorsa ve önceki **Özel Yükleme durumunda - Bileşen Seçimi** iletişim kutusunda **Uzaktan yönetim** ögesini yüklenecek olarak işaretlediyseniz, **AVG DataCenter** parametrelerini belirtmeniz gerekir:



AVG DataCenter belirtimi metin alanına **AVG DataCenter** bağlantı dizisini *sunucu: bağlantı noktası* biçiminde girin. Bu bilgi o anda yoksa, alanı boş bırakın ve yapılandırmayı [Gelişmiş Ayarlar / Uzaktan Yönetim](#) iletişim kutusu içinde daha sonra

ayarlayabilirsiniz.

Not: AVG Uzaktan yönetim hakkında ayrıntılı bilgiler için, AVG Network Edition kullanıcı kılavuzuna başvurun; AVG web sitesinden (<http://www.avg.com/>) indirilebilir.

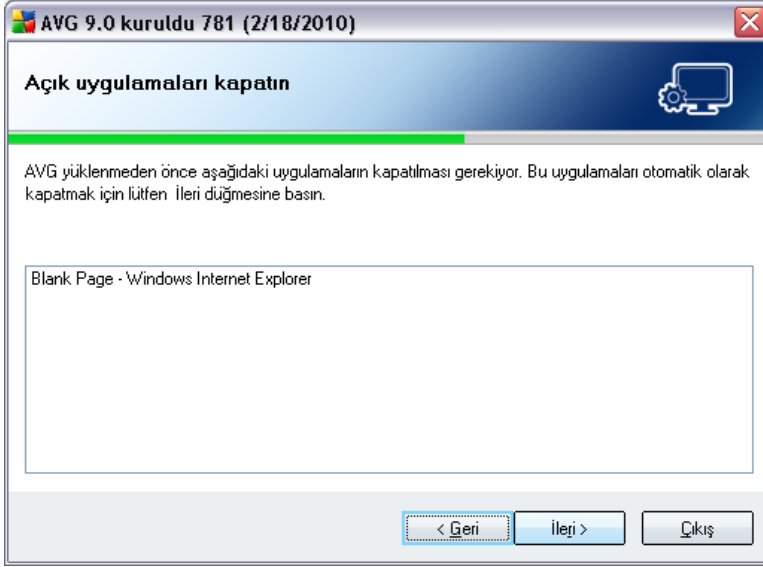
5.9. AVG Security Toolbar



AVG Security Toolbar iletişim kutusunda, **AVG Security Toolbar**'i yüklemek isteyip istemediğinize karar verin (*Desteklenen Internet arama motorlarının arama sonuçlarının doğrulaması*). Varsayılan ayarları değiştirmeden, Internet'te gezinirken size daha kapsamlı koruma sağlamak için bu bileşen otomatik olarak Internet tarayıcınıza yüklenir (*geçerli olarak desteklenen tarayıcılar Microsoft Internet Explorer v. 6.0 veya daha üstü ve Mozilla Firefox v. 2.0 veya daha üstüdür*).

Ayrıca, Yahoo! 'yu varsayılan arama motorunuz olarak ayarlama seçeneğiniz de vardır. Öyleyse, lütfen ilgili onay kutusunu işaretleyin.

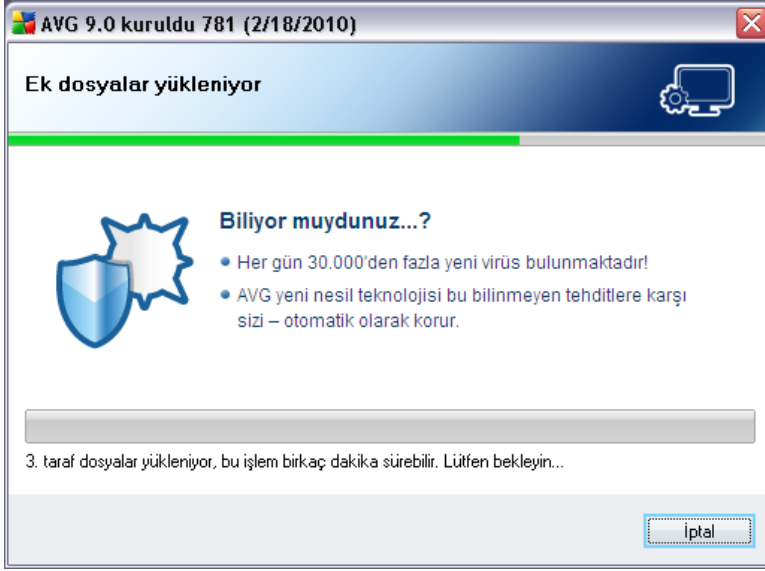
5.10. Açık uygulamaları kapatın



Açık uygulamaları kapat iletişim kutusu, yükleme işleminde yalnızca bilgisayarınızda o anda çalışan başka çakışan programlar olduğunda görünür. Sonra, başarılı bir şekilde yükleme işlemini bitirmek için kapatılması gereken programların listesi sağlanacaktır. İlgili uygulamaların kapatılmasını kabul etmeyi onaylamak ve bir sonraki adımla devam etmek için **İleri** düğmesine basın.

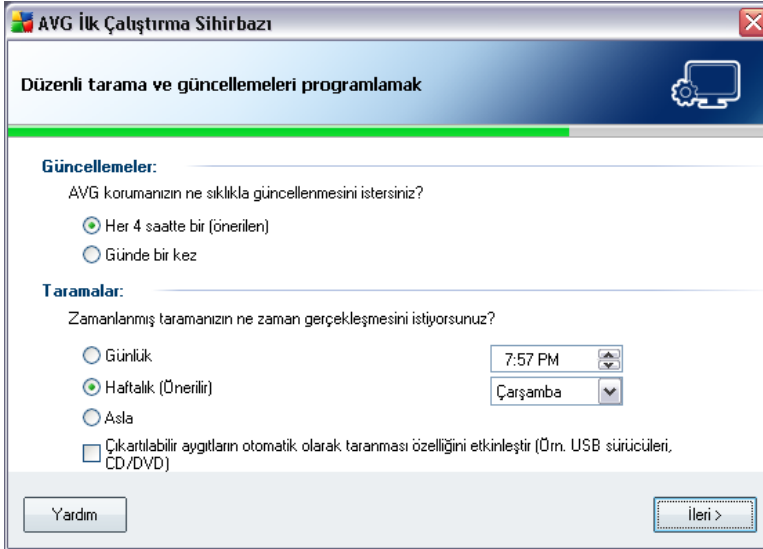
5.11. AVG Yükleniyor

AVG Yükleniyor iletişim kutusunda yükleme işleminin ilerleme durumu görüntülenir ve herhangi bir müdahale gerektirmez:



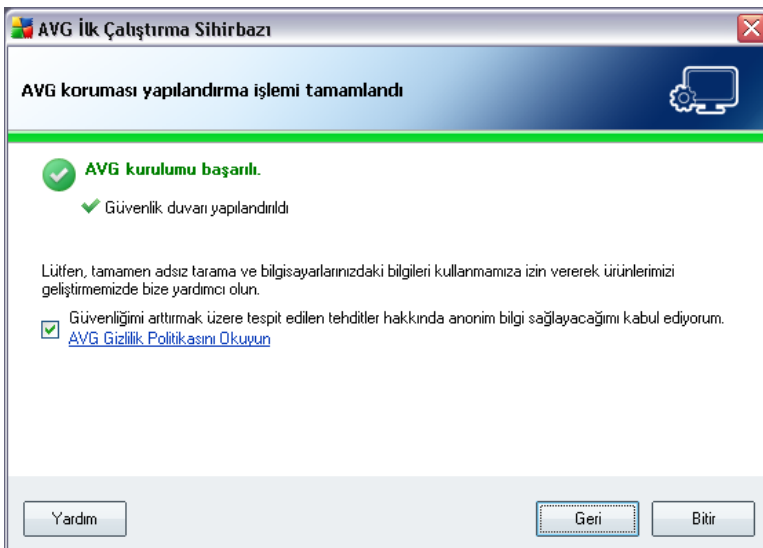
Yükleme işlemi bittiginde, bir sonraki iletişim kutusuna otomatik olarak yönlendirileceksiniz.

5.12. Düzenli tarama ve güncellemeleri programlamak



Düzenli tarama ve güncellemeleri planla iletişim kutusunda yeni güncelleme dosyalarına erişim kontrolleri için zaman aralıkları belirleyebilir ya da [planlanan taramanın](#) saat kaçta baslatılacağını girebilirsiniz. Varsayılan değerleri muhafaza etmeniz önerilir. Devam etmek için **İleri** düğmesini tıklayın.

5.13. AVG koruması yapılandırması tamamlandı





AVG 9 Anti-Virus ürününüz şimdi yapılandırıldı.

Bu iletişim kutusunda, bilinmeyen açıklardan yararlanma raporunu ve kötü siteleri AVG virüs laboratuvarına bildirme seçeneğini etkinleştirmek isteyip istemediğinize karar verirsiniz. İstiyorsanız, lütfen **Güvenligimi geliştirmek için algılanan tehlikeler hakkında ADSIZ olarak bilgiler sağlamayı kabul ediyorum** seçeneğini işaretleyin.

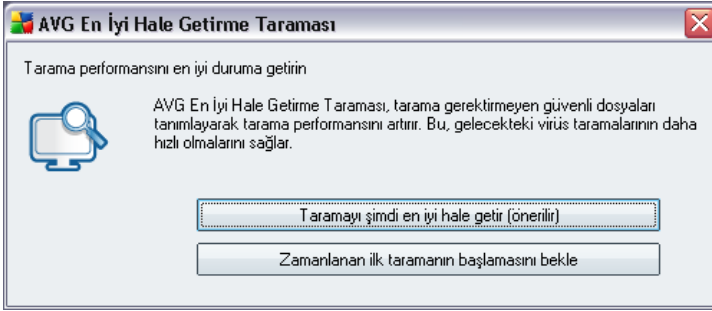
Son olarak, **Son** düğmesine basın.

6. Yüklemeden Sonra

6.1. Taramayı en iyi hale getirme

Taramayı en iyi duruma getirme işlevi, uygun dosyaları algıladığı yerde *Windows* ve *Program dosyaları* klasörlerini arar (o anda, bunlar *.exe, *.dll ve *.sys dosyalarıdır) ve bu dosyalardaki bilgileri kaydeder. Bir sonraki erişimde, bu dosyalar bir daha taranmaz ve bu, tarama süresini önemli ölçüde azaltır.

Yükleme işlemi bittiginde taramayı en iyi duruma getirmek için yeni bir iletişim kutusu penceresiyle davet edilirsiniz:



Bu seçeneği kullanmanızı ve ***Taramayı şimdi en iyi duruma getir*** düğmesine basarak taramayı en iyi duruma getirme işlemini çalıştırmanızı öneririz.

6.2. Ürün Kaydı

AVG 9 Anti-Virus yüklemesini bitirdikten sonra, lütfen ürününüzü AVG web sitesinin (<http://www.avg.com/>), **Kayıt** sayfasından kaydedin (*doğrudan sayfada verilen yönergeleri izleyin*). Kayıt işleminin ardından AVG Kullanıcı hesabınıza erişebilecek, AVG Güncelleme bültenini alacak ve sadece kayıtlı kullanıcılara sunulan diğer hizmetlerden yararlanacaksınız.

6.3. Kullanıcı Arayüzü'ne Eriş

AVG Kullanıcı Arayüzü'ne çeşitli şekillerde ulaşabilirsiniz:

- sistem tepsisindeki AVG simgesine çift tıklatın
- masaüstünüzdeki AVG simgesine çift tıklatın

- **Baslat/Programlar/AVG 9.0/AVG Kullanici Arayüzü menüsünden**

6.4. Tam bilgisayar taraması

AVG 9 Anti-Virus yüklemesinden önce bilgisayarınıza virüs bulasmis olmasi ihtimali bulunmaktadır. Bu nedenle bilgisayarınızda virüs bulunmadigindan emin olmak için [Tam bilgisayar taramasi](#) yapmanız gerekmektedir.

[Tam bilgisayar taramasi](#) konusunda talimatlar için lütfen [AVG Taramasi](#) bölümünü inceleyin.

6.5. Eicar Testi

AVG 9 Anti-Virus programinin düzgün olarak yüklendigini onaylamak için EICAR testini çalistirabilirsiniz.

EICAR testi, virüsten koruma sistemin çalistigindan emin olmak üzere kullanılan standart ve kesinlikle güvenli bir yöntemdir. Gerçek bir virüs olmadigi için yayilmasinda sakınca yoktur ve herhangi bir virüs kodu içermemektedir. Ürünlerin çoğu sanki bir virüsmüs gibi tepki verir (*ancak "EICAR-AV-Test" adi altında rapor ederler*). EICAR virüsünü www.eicar.com adresinde bulunan EICA'in web sitesinden indirebilir ve bunun yani sıra EICAR testi hakkında tüm gerekli bilgileri edinebilirsiniz.

eicar.com dosyasini indirmeye çalisin ve sabit diskinize kaydedin. Test dosyasinin indirme islemini onaylar onaylamaz, [Online Shield](#) bir uyarıyla virüse tepki verecektir. Bu bildirim, AVG'nin bilgisayarınıza dogru bir sekilde yüklenmis oldugunu gösterir.



<http://www.eicar.com> web sitesinden EICAR 'virüs' sikistirilmis sürümünü (örn. *eicar_com.zip biçiminde*) de indirebilirsiniz. [Online Shield](#), bu dosyayi indirmenizi ve



yerel diskinize kaydetmenizi sağlar, ancak [Yerlesik Kalkan](#) paketi açmaya çalıştığınızda 'virüs' algılar. **AVG'nin EICAR test dosyasını virüs olarak algılamaması halinde program yapılandırmasını yeniden kontrol etmeniz gerekir!**

6.6. AVG Varsayılan Yapılandırması

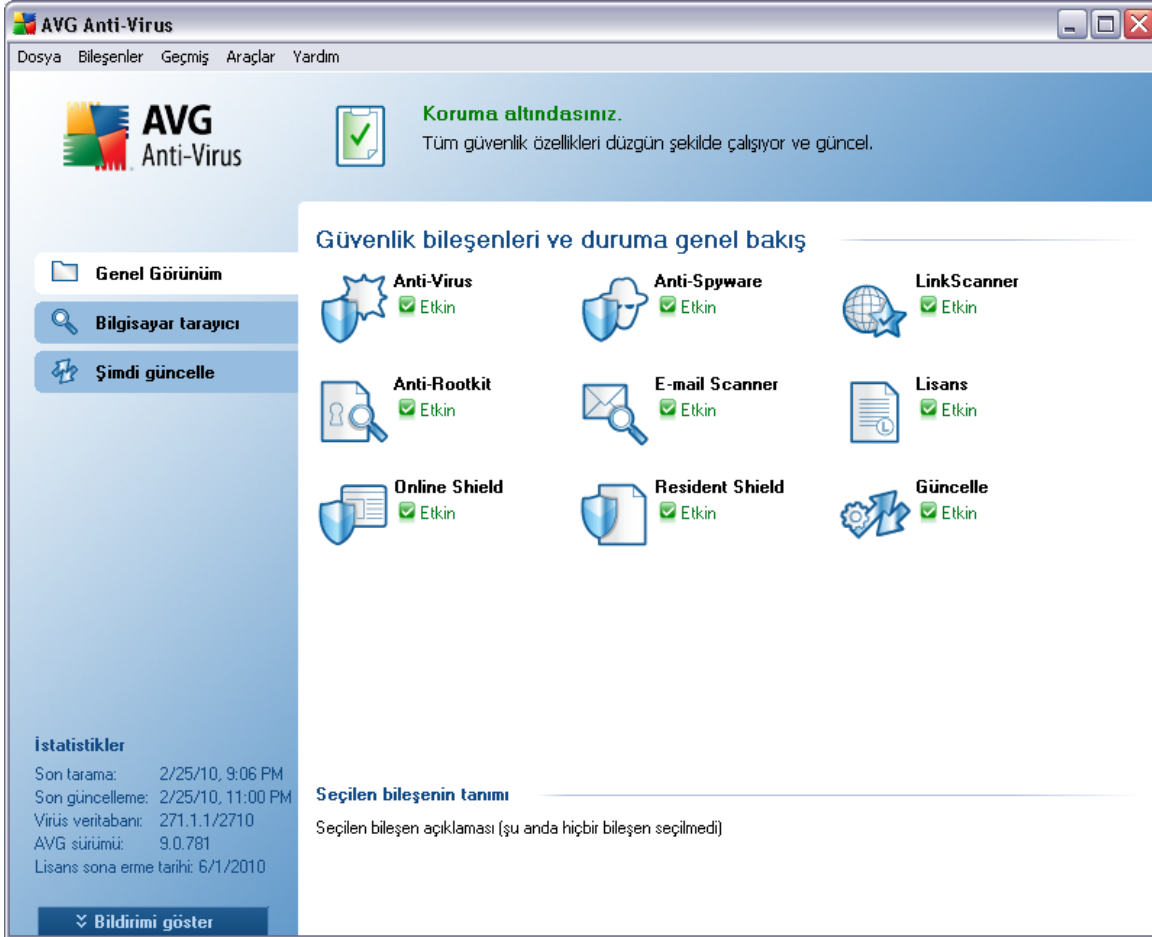
AVG 9 Anti-Virus varsayılan yapılandırması (örn. uygulamanın yükledikten sonra doğru şekilde nasıl ayarlanacağı) yazılım satıcısı tarafından ayarlanabilir, böylece optimum performans elde etmek için tüm bileşenler ve işlevler ayarlanabilir.

Bunun için iyi bir nedeniniz olmadıkça AVG yapılandırmasını değiştirmeyin! Ayarlarda yapılacak her tür değişiklik sadece deneyimli bir kullanıcı tarafından gerçekleştirilmelidir.

[AVG bileşenlerinde](#) yapılan bazı ufak değişikliklere ilgili bileşenin kullanıcı arayüzünden ulaşabilirsiniz. İhtiyaçlarınızı daha iyi karşılaması açısından AVG yapılandırmasını değiştirme ihtiyacı hissederseniz [AVG Gelismis Ayarları](#)'na gidin: sistem menüsü öğesini seçin **Araçlar/Gelismis ayarlar** ve AVG yapılandırmasını yeni açılan [AVG Gelismis Ayarlar](#) penceresinde düzenleyin.

7. AVG Kullanıcı Arayüzü

AVG 9 Anti-Virus, ana pencerede açılır:



Ana pencere çok sayıda bölüme ayrılır:

- **Sistem Menüsü** (penceredeki en üst sistem çubuğu) tüm AVG bileşenlerine, servislerine ve özelliklerine ulaşmanızı sağlayan standart dolanım yöntemidir - [ayrıntılar >>](#)
- **Güvenlik Durumu Bilgileri** (pencerenin üst bölümü) AVG programının mevcut durumu hakkında bilgi sunar - [ayrıntılar >>](#)
- **Hızlı Bağlantılar** (pencerenin sol bölümü) en önemli ve en sık kullanılan AVG görevlerine hızlı bir şekilde erişebilmenizi sağlar - [ayrıntılar >>](#)

- **Bileşenlere Genel Bakış** (pencerenin orta kısmı) yüklü AVG bileşenleri hakkında genel bilgi verir - [ayrıntılar >>](#)
- **İstatistikler** (pencerenin sol alt kısmı) programın çalışmasına ilişkin istatistik verileri görüntüler - [ayrıntılar >>](#)
- **Sistem Tepsisi Simgesi** (ekranın sağ alt köşesi, sistem tepsisi üzerinde) AVG'nin mevcut durumunu gösterir - [ayrıntılar >>](#)

7.1. Sistem Menüsü

Sistem menüsü tüm Windows uygulamalarında kullanılan standart bir dolanım yöntemidir. **AVG 9 Anti-Virus** ana penceresinin en üstünde yatay olarak konumlandırılmıştır. Belirli AVG bileşenlerine, özelliklerine ve hizmetlerine ulaşmak için sistem menüsünü kullanın.

Sistem menüsü beş ana bölüme ayrılmıştır:

7.1.1. Dosya

- **Çıkış** - **AVG 9 Anti-Virus**'nin kullanıcı arayüzünü kapatır. Ancak AVG uygulaması arkaplanda çalışmaya devam edecek ve bilgisayarınız korunmaya devam edecektir.

7.1.2. Bileşenler

Sistem menüsünün **Bileşenler** ögesi, yüklenen tüm AVG bileşenlerine ilişkin bağlantılar içerir ve kullanıcı arayüzünde varsayılan iletişim kutularını açar.

- **Sisteme genel bakış** - [Yüklenen bileşenler ve durumlarına ek olarak varsayılan kullanıcı arayüzü iletişim kutusuna geçer](#)
- **Virüsten Koruma** - [Virüsten Koruma](#) bileşeninin varsayılan sayfasını açar
- **Rootkit Önleme** - [Rootkit Önleme](#) bileşeninin varsayılan sayfasını açar
- **Casus Yazılımından Koruma** - [Casus Yazılımından Koruma](#) bileşeninin varsayılan sayfasını açar
- **Link Scanner** - [Link Scanner](#) bileşeninin varsayılan sayfasını açar
- **E-posta tarayıcısı** - [E-posta Tarayıcısı](#) bileşeninin varsayılan sayfasını açar
- **Lisans** [Lisans](#) bileşeninin varsayılan sayfasını açar

- **Online Shield** - [Online Shield](#) bileşeninin varsayılan sayfasını açar
- **Yerlesik Kalkan** - [Yerlesik Kalkan](#) bileşeninin varsayılan sayfasını açar
- **Güncelleme Yöneticisi** - [Güncelleme Yöneticisi](#) bileşeninin varsayılan sayfasını açar

7.1.3. Geçmiş

- [Tarama sonuçları](#) - AVG test arayüzüne özellikle [Tarama Sonuçlarına Genel Bakış](#) penceresine gider
- [Yerlesik Kalkan Tespiti](#) - [Yerlesik Kalkan](#)
- [E-posta Tarayıcısı Tespiti](#) - [E-posta Tarayıcısı](#) bileşeni tarafından tehlikeli olduğu tespit edilen posta eklentileri hakkında genel bilgi veren bir iletişim kutusu açar
- [Online Shield Tespitleri](#) - [Online Shield](#)
- [Virüs Kasası](#) - Belirli bir neden doğrultusunda AVG'nin tespit edilmiş temizlenemeyen tüm bulasmaları sildiği karantina alanının arayüzünü açar ([Virüs Kasası](#)) Karantina altında bulunan bulasmis dosyalar, yalıtılmıştır, bilgisayarınızın güvenliği garanti altındadır ve aynı anda bulasmis dosyalar ileride tamir edilebilecekleri göz önünde bulundurularak depolanır.
- [Etkinlik Geçmişi Kayıt Defteri](#) - kaydedilen **AVG 9 Anti-Virus** eylemlerin tümü hakkında genel bilgi veren bir pencere açar.

7.1.4. Araçlar

- [Bilgisayarı tara](#) - [AVG tarama arayüzüne](#) geçer ve tüm bilgisayar taramasını başlatır
- [Seçilen klasörü tara](#) - [AVG tarama arayüzüne](#) geçer ve bilgisayarınızın dolasımlarından taranmasını istediğiniz dosya ve klasörleri seçmenizi sağlar
- [Dosyayı tara](#) - sabit diskinizin dolasımlarından seçtiğiniz tek bir dosyayı isteğe bağlı olarak tarayabilmenizi sağlar
- [Güncelle](#) - otomatik olarak **AVG 9 Anti-Virus**
- [Dizinden güncelle](#) - sabit diskinizde bulunan belirli bir dosyanın içinde yer alan güncelleme dosyalarını alarak güncelleme işlemini gerçekleştirir. Diğer bir yandan bu seçim sadece acil durumlarda önerilmektedir. Örn. İnternet bağlantısı olmadığı

durumlarda (Örneğin bilgisayarınıza virüs bulaşmış ise ve Internet bağlantınız kesildiyse; bilgisayarınız bir ağa bağlıysa fakat Internet erişimi yok ise, vb.). Yeni açılan pencereden, daha önce güncelleme dosyasını depoladığınız klasörü seçin ve güncelleme işlemini başlatın.

- **Gelismis ayarlar** - _yapilandirmasını düzenleyebileceğiniz **AVG 9 Anti-Virus** **AVG gelişmiş ayarlar** iletişim kutusunu açar. Genel olarak uygulamanın yazılım üreticisi tarafından tanımlanan öntanımlı ayarlarının muhafaza edilmesi önerilir.

7.1.5. Yardım

- **İçindekiler** - AVG yardım dosyalarını açar
- **Çevrimiçi Yardım Alın** - Müşteri destek merkezi sayfasında AVG web sitesini (<http://www.avg.com/>) açar
- **AVG Web** - AVG web sitesini (<http://www.avg.com/>) açar
- **Virüsler ve Tehditler Hakkında** - tanımlanan virüs hakkında ayrıntılı bilgi edinebildiğiniz **Virüs Ansiklopedisini** açar
- **Yeniden Etkinleştir** - **Yükleme işleminin AVG'yi Kisiselleştir** iletişim kutusuna girilen verilerle **AVG'yi Etkinleştir** iletişim kutusunu açar. Bu iletişim kutusunda satış numaranızı (AVG'yi yüklerken kullandığınız numara), ya da eski lisans numaranızı (Örn. yeni bir AVG ürününe geçerken) değiştirmek için lisans numaranızı girebilirsiniz.
- **Simdi kaydolan** - AVG web sitesi (<http://www.avg.com/>) kayıt sayfasına bağlanır. Lütfen kayıt bilgilerinizi doldurun; sadece AVG ürünlerini kaydettiren müşterilerimiz ücretsiz teknik destek alabilecektir.

Not: AVG 9 Anti-Virus deneme sürümünü kullanıyorsanız, sonraki iki öge, **Simdi satın al ve **Etkinleştir** olarak görünür, programın tam sürümünü hemen satın almanızı sağlar. Bir satış numarasıyla yüklenmiş **AVG 9 Anti-Virus** için, öğeler **Kaydet** ve **Etkinleştir** olarak görünür. Daha fazla bilgi için, lütfen bu dokümantasyonun **Lisans** kısmına başvurun.**

- **AVG Hakkında** - **AVG Technologies CZ**'nin iletişim bilgileri, lisans sözleşmesi, sistem bilgileri, program ve virüs veritabanı versiyonu ve program adı hakkında bilgi veren bes sekmeli **Bilgi** iletişim kutusunu açar.

7.2. Güvenlik Durumu Bilgisi

Güvenlik Durumu Bilgisi bölümü, AVG'nin ana penceresinin üst kısmında bulunmaktadır. Bu bölümde **AVG 9 Anti-Virus** programınızın mevcut güvenlik durumu hakkında her zaman bilgi bulabilirsiniz. Lütfen bu bölümde betimlenmesi muhtemel simgeleri ve anlamlarını inceleyin:



Yesil simge AVG'nizin tamamen fonksiyonel olduğunu gösterir. Bilgisayarınız tamamen korunur, günceldir ve yüklü tüm bileşenler doğru çalışmaktadır.



Turuncu simge, bir ya da daha fazla bileşenin yanlış yapılandırıldığını ve söz konusu bileşenlerin özelliklerine/ayarlarına dikkat etmeniz gerektiğini gösterir. AVG'de herhangi bir kritik sorun yoktur ve muhtemelen bir nedenden dolayı bileşenlerden bazılarını geçici olarak kapatmayı seçmiş olabilirsiniz. Ancak AVG tarafından korunmaya devam edersiniz. Diğer bir yandan lütfen bileşenin ayarlarını inceleyin! Adı **Güvenlik Durumu Bilgisi** kısmında sağlanır.

Bu simge, herhangi bir nedenle [bir bileşenin hata durumunu göz ardı etmeyi seçtiyseniz](#) de görüntülenecektir ("*Bileşen durumunu göz ardı et*" seçeneğine, AVG ana penceresinin bileşenlere genel bakış kısmında bulunan ilgili simgeyi sağ tıklayarak açtığınız bağlam menüsünden ulaşabilirsiniz). Özel durumlar için bu seçeneği kullanmanız gerekebilir ancak en kısa zamanda **Bileşen durumunu gözardı et** seçeneğini devre dışı bırakmanız önerilir.



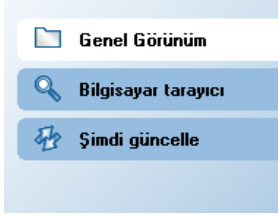
Kırmızı simge, AVG'nin kritik durumda olduğunu gösterir! Bir ya da daha fazla bileşen doğru çalışmıyor ve AVG bilgisayarınızı koruyamıyor anlamına gelir. Lütfen rapor edilen sorunu çözmek için gerekli ilgiyi gösterin. Hatayı kendi başınıza çözemezseniz [AVG teknik destek](#) ekibi ile iletişim kurun.

Güvenlik Durumu Bilgisi fonksiyonuna gereken özeni göstermeniz ve herhangi bir sorunun rapor edilmesi halinde anında sorunu çözmeye çalışmanız önerilmektedir. Aksi takdirde bilgisayarınız risk altında olacaktır!

Not: AVG durum bilgilerine [sistem tepsisi simgesinden](#) de ulaşabilirsiniz.

7.3. Hızlı Bağlantılar

Hızlı Bağlantılar ([AVG Kullanıcı Arayüzü](#)'nın sol kısmında) en sık kullanılan ve en önemli AVG özelliklerine hemen erişebilmenizi sağlar:



- **Genel Bakis** - açık durumdaki herhangi bir AVG arayüzünden yüklü bileşenlerin tümünün görüntüldüğü genel bakis penceresine gitmek için bu bağlantıyı kullanın - bkz. bölüm [Bileşenlere Genel Bakis >>](#)
- **Bilgisayar taraması** - taramaları doğrudan başlatabildiğiniz, tarama programlayabildiğiniz ya da parametreleri değiştirebildiğiniz AVG tarama arayüzünü açmak için bu bağlantıyı tıklayın - bkz. bölüm [AVG Taramaları >>](#)
- **Şimdi güncelle** -bu bağlantı güncelleme arayüzünü açacak ve AVG güncelleme işlemini başlatacaktır - bkz. bölüm [AVG Güncellemeleri >>](#)

Bu bağlantılara kullanıcı arayüzünden istediğiniz zaman ulaşabilirsiniz. Belirli bir işlemi başlatmak üzere hızlı bağlantılardan birini kullandığınızda GUI yeni bir iletişim kutusunda açılacaktır fakat söz konusu iletişim kutusundan da hızlı bağlantılara ulaşabilirsiniz. Buna ek olarak çalışan işlem grafiksel olarak da betimlenmektedir.

7.4. Bileşen Genel Görünümü

Bileşenlere Genel Bakis bölümü [AVG Kullanıcı Arayüzü](#)'nın orta kısmında yer alır. Bölüm ikiye ayrılır:

- Yanlarında bileşenin simgesinin ve aktif ya da pasif olduğuna dair durum bilgisinin bulunduğu yüklü tüm bileşenlere genel bakis
- Seçilen bileşen hakkında açıklamalar

AVG 9 Anti-Virus içinde, **Bileşen Genel Görünümü** kısmi aşağıdaki bileşenler hakkında bilgiler içerir:

- **Virüsten Koruma** , bilgisayarınızı bilgisayarınıza girmeye çalışan virüslerden korur - [ayrıntılar >>](#)

- **Casus Yazilimdan Koruma** siz çalistirdikça uygulamalarinizi arkaplanda tarar - [ayrintilar >>](#)
- **LinkScanner** Internet tarayicisinde görüntülenen arama sonuçlarini kontrol eder- [ayrintilar >>](#)
- **Rootkit Önleme** zararli yazilimlari gizlemeye çalisan program ve teknolojileri tespit eder - [ayrintilar >>](#)
- **E-posta Tarayicisi** gelen ve giden postalari virüslere karsi kontrol eder - [ayrintilar >>](#)
- **Lisans**, lisans numarasini, türünü ve son kullanma tarihini görüntüler - [ayrintilar >>](#)
- **Online Shield** bir web tarayicisi tarafından indirilen tüm verileri tarar - [ayrintilar >>](#)
- **Yerlesik Kalkan** arkaplanda çalisir ve dosyalar kopyalanir, açilir ve kaydedilirken söz konusu dosyalari tarar - [ayrintilar >>](#)
- **Güncelleme Yöneticisi** tüm AVG güncellemelerini kontrol eder - [ayrintilar >>](#)

Bilesenlere genel bakis ekraninda bileseni seçmek için üzerine bir defa tiklatin. Ayni anda kullanıcı arayüzünün alt kisminda bilesenin temel fonksiyonlari hakkında açıklamalar görüntülenir. Bilesenin kendi arayüzünü açmak ve temel istatistiki verileri görüntülemek için simgeye çift tiklatin.

Bir baglam menüsü açmak için bilesenin simgesi üzerine sag tiklatin: bilesenin grafik arayüzünü açmanın yani sıra **Bilesenin durumunu göz ardi et** seçimini de yapabilirsiniz. [Bilesenin hata durumunun](#) bilincinde olduğunuzu göstermek için bu seçenegi seçin, ancak belirli bir neden doğrultusunda AVG'nizin bu şekilde çalışmasını istiyorsanız [sistem tepsisi simgesi](#) ile uyarılmayacaksınız.

7.5. İstatistikler

İstatistikler bölümü [AVG Kullanıcı Arayüzü](#)'nün sol alt kisminda yer alır. Programın çalışması hakkında bir dizi bilgi içerir:

- **Son tarama** - son taramanın yapıldığı tarihi gösterir
- **Son güncelleme** - son güncellemenin yapıldığı tarihi gösterir
- **Virüs VT** - mevcut virüs tabanı sürümü hakkında bilgi verir

- **AVG sürümü** - yüklü AVG sürümü hakkında bilgi verir (*numara 9.0.xx formatındadır ve burada 9.0 ürün sürümü iken xx üretim numarasını gösterir*)
- **Lisansin son kullanilma tarihi** - AVG lisansinizin son kullanilma tarihini gösterir

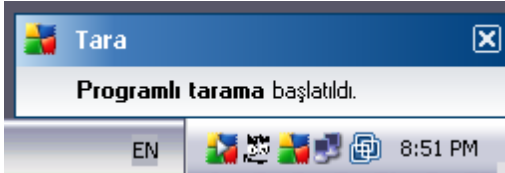
7.6. Sistem Tepsisi Sembolü

Sistem Tepsisi Sembolü (Windows araç çubuğunda), **AVG 9 Anti-Virus** programınızın geçerli durumunu gösterir. AVG ana penceresinin açık ya da kapalı olduğu önemli olmaksızın devamlı olarak sistem tepsiniz üzerinde bulunur.

Tamamen renkli ise  **Sistem Tepsisi Sembolü**, tüm AVG bileşenlerinin aktif ve tamamen fonksiyonel olduğunu gösterir. Buna ek olarak AVG hata durumundayken de AVG sistem tepsisi sembolü tamamen renkli görüntülenebilir, ancak bu, durumun tamamen farkındasınız ve bilerek [Bileşen durumunu gözardı et](#) seçimini yapmışınız demektir.

Ünlem isareti içeren bir simge  bir sorun olduğunu gösterir (*etkin olmayan bileşen, hata durumu vb.*). Ana pencereyi açmak ve bileşeni düzenlemek için **Sistem Tepsisi Sembolünü** çift tıklatın.

Sistem tepsisi sembolü geçerli AVG etkinlikleri ve programdaki olası durum değişiklikleri (örn. programlanmış bir taramanın veya güncellemenin otomatik başlatılması, bir bileşenin durumundaki değişiklik, hata durumu oluşumları...), AVG sistem tepsisi sembolünde açılır bir pencere yoluyla hakkında bilgi de verir:



Sistem Tepsisi Sembolü AVG ana penceresine istediğiniz zaman ulaşabilmeniz için hızlı bir bağlantı olarak da kullanılabilir - sadece simgeyi iki defa tıklatın. **Sistem Tepsisi Sembolü** sağ tıklayarak aşağıdaki seçenekleri sunan kısa bir bağlam menüsü açarsınız:

- **AVG Kullanıcı Arayüzünü Aç** - [AVG Kullanıcı Arayüzünü açmak için tıklatın](#)
- **Güncelle** - anında [güncelleme işlemini başlatır](#)



8. AVG Bileşenleri

8.1. Virüsten Koruma

8.1.1. Virüsten Koruma İlkeleri

Antivirüs yazılımlarının tarama motorları bilinen tüm virüslere karşı tüm dosya ve dosya işlemlerini (dosyaların açılması/kapatılması, vb) tarar. Tespit edilen virüsler, harekete geçmeden engellenecek ve ardından silinecek ya da karantinaya alınacaktır. Antivirüs yazılımlarının çoğu bulgusal taramayı kullanır; diğer bir deyişle, dosyalar virüs imzası olarak adlandırılan tipik virüs özelliklerine karşı taranır. Bu, yeni bir virüs mevcut virüslerin tipik özelliklerinden bazılarına sahipse söz konusu antivirüs tarayıcısının yeni ve bilinmeyen bir virüsü tespit edebileceği anlamına gelmektedir.

Antivirüs korumasının en önemli özelliği, bilgisayarınıza hiçbir virüsün bulasmamasının sağlanmasıdır!

Tek bir teknoloji bir virüsün tespit edilmesinde ya da tanımlanmasında yetersiz kalabileceken **Anti-Virus**, bilgisayarınızın virüslerden korunduğundan emin olmak adına çok sayıda teknolojiyi bir araya getirmektedir:

- Tarama - belirli bir virüsün özelliklerine sahip karakter komut satırları aranır
- Bulgusal analiz - sanal bir bilgisayar ortamında taranan nesnenin ' komutları dinamik bir şekilde canlandırılır
- Jenerik tespit - belirli bir virüs ya da virüs grubunun komut özelliklerinin tespitidir

AVG bunun yanı sıra sistemde potansiyel anlamda istenmeyen çalıştırılabilir uygulamaları ya da DLL kütüphanelerini de inceleyebilmekte ve tespit edebilmektedir. Söz konusu tehditleri Potansiyel Olarak İstenmeyen Programlar (farklı casus yazılım, reklam yazılım türleri, vb) olarak adlandırıyoruz. Buna ek olarak AVG, bilgisayarınızı şüpheli girdilere, geçici İnternet Dosyalarına ve izleme çerezlerine karşı da tarar ve söz konusu potansiyel olarak istenmeyen nesneleri de diğer bulasmalarla aynı şekilde çözebilmenize olanak tanır.

8.1.2. Virüsten Koruma Arayüzü



Anti-Virus bileşeninin arayüzünde bileşenin fonksiyonlarına, bileşenin mevcut durumu hakkında bilgiye (*Anti-Virus bileşeni aktiftir.*) ve **Anti-Virus** istatistikleri hakkında kısa bilgilere ulaşabilirsiniz.

- **Bulasma tanımları** - Sayı, virüs veritabanının güncel sürümünde tanımlanan virüs sayısını gösterir.
- **En son veritabanı güncelleme** - virüs veritabanının en son güncellendiği tarih ve saati gösterir.
- **Veritabanı sürümü**- en son virüs veritabanı sürümünün numarasını tanımlar ve bu numara virüs veritabanı her güncellendiğinde artar

Bu bileşenin arayüzü kapsamında sadece bir adet çalıştırma düğmesi bulunur (**Geri**) - Varsayılan [AVG Kullanıcı Arayüzüne](#) dönmek için bu düğmeye basın (bileşenlere genel bakış).

Lütfen dikkat: Yazılım satıcısı, en iyi performansın sunulabilmesi için tüm AVG bileşenlerini kurmuştur. Bunun için iyi bir nedeniniz olmadıkça AVG yapılandırmasını

degistirmeyin. Ayarlarda yapılacak her tür degisiklik sadece deneyimli bir kullanıcı tarafından gerçekleştirilmelidir. AVG yapılandırmasını degistirmeniz gerekiyorsa sistem menüsünden ilgili öğeyi seçin **Araçlar/Gelismis ayarlar** ve yeni açılan [AVG Gelismis Ayarlar](#) iletişim kutusunda AVG yapılandırmasını düzenleyin.

8.2. Casus Yazılımdan Koruma

8.2.1. Casus Yazılımdan Koruma Prensipleri

Casus yazılımlar, genellikle kullanıcının bilgisi ya da izni olmaksızın kullanıcının bilgisayarından bilgi toplayan zararlı bir yazılım türü olarak tanımlanırlar. Bazı casus yazılım uygulamaları genellikle belirli bir amaç doğrultusunda kurulur ve sıklıkla reklam, açılan pencereler veya farklı istenmeyen yazılım türleri içerirler.

Su anda bilinen en yaygın bulaşma kaynağı, potansiyel anlamda tehlikeli öğeler içeren web siteleridir. E-posta ya da solucan ve virüsler yoluyla aktarım gibi diğer bulaşma yöntemleri de oldukça etkilidir. En önemli korunma, yerleşik bir kalkan olarak çalışan ve siz çalıştığınız zaman arka planda uygulamalarını tarayan **Anti-Spyware** gibi devamlı olarak arka planda çalışan bir tarayıcı kullanmaktır.

Kötü amaçlı yazılımın bilgisayarınıza AVG yüklenmesinden önce bulaşmış olması ya da **AVG 9 Anti-Virus** programınızı en güncel [veritabanı ve program güncellemeleriyle güncel tutmayı ihmal etmeniz gibi potansiyel riskler de bulunmaktadır](#). Bu nedenle AVG, tarama özelliğini kullanarak tüm bilgisayarınızı zararlı ve casus yazılımlara karşı tarayabilmenize olanak tanır. Ayrıca, uykuda olan ve etkin olmayan kötü niyetli yazılımları da (örneğin bilgisayara indirilmiş ancak henüz etkinleştirilmemiş) tespit eder.

8.2.2. Casus Yazılımdan Koruma Arayüzü



Anti-Spyware bileşeninin arayüzünde bileşenin fonksiyonlarına, bileşenin mevcut durumu hakkında bilgiye (*Anti-Spyware bileşeni aktiftir.*) ve bazı **Anti-Spyware** istatistiklerine ulaşabilirsiniz:

- **Casus yazılım tanımları** - Sayı, en güncel casus yazılım veri tabanı sürümünde tanımlanan casus yazılım örneği sayısını gösterir.
- **En son veritabanı güncelleme** - casus yazılım veritabanının en son güncellendiği tarih ve saati gösterir.
- **Veritabanı sürümü**- en son casus yazılım veritabanı sürümünün numarasını tanımlar ve bu numara virüs veritabanı her güncellendiğinde artar

Bu bileşenin arayüzü kapsamında sadece bir adet çalıştırma düğmesi bulunur (**Geri**) - Varsayılan [AVG Kullanıcı Arayüzüne](#) dönmek için bu düğmeye basın (bileşenlere genel bakış).

Lütfen dikkat: Yazılım satıcısı, en iyi performansın sunulabilmesi için tüm AVG bileşenlerini kurmustur. Bunun için iyi bir nedeniniz olmadıkça AVG yapılandırmasını

degistirmeyin. Ayarlarda yapılacak her tür degisiklik sadece deneyimli bir kullanıcı tarafından gerçekleştirilmelidir. AVG yapılandırmasını degistirmeniz gerekiyorsa sistem menüsünden ilgili öğeyi seçin **Araçlar/Gelismis ayarlar** ve yeni açılan [AVG Gelismis Ayarlar](#) iletişim kutusunda AVG yapılandırmasını düzenleyin.

8.3. Rootkit Önleme

Rootkit, sistem yöneticisinin izni olmaksızın yasal olmayan şekillerde bilgisayar sisteminin kontrolünü ele almak için tasarlanmış bir programdır. Kök kullanıcı, donanım üzerinde çalışan işletim sisteminin kontrolünü ele geçirmeyi hedeflediği için donanımsal açıdan erişime gerek duymaz. Genellikle kök kullanıcılar, standart işletim sistemi güvenlik mekanizmalarını dönüştürerek ya da istila ederek sistem üzerindeki varlıklarını gizlerler. Sıklıkla Truva Ati biçimindedirler, dolayısıyla kullanıcıları sistemleri üzerinden çalışacak kadar güvenli olduklarına inandırır. İzleme programlarının çalışan işlemlerini gizlemek ya da işletim sisteminin sistem bilgilerini ya da dosyalarını saklamak, bunu sağlamak için kullanılan teknikler arasında bulunmaktadır.

8.4. E-Posta Tarayıcısı

Virüsler ve truva atları yaygın olarak e-postalar aracılığıyla yayılır. Yemleme ve istenmeyen postalar, e-postaları daha büyük risk kaynakları haline getirmektedir. Ücretsiz e-posta hesaplarının zararlı e-postaları alma ihtimali daha yüksek olup (*nadiren istenmeyen posta önleme teknolojilerine sahip olmaları nedeniyle*) ev kullanıcıları büyük çoğunlukla söz konusu e-postaları kullanır. Bunun yanı sıra, bilmedikleri sitelerde dolan ve çevrimiçi formları kişisel bilgileri ile dolduran (*e-posta adresleri gibi*) ev kullanıcıları, e-posta saldırılarına sıklıkla maruz kalmaktadır. Şirketler genellikle kurumsal e-posta hesapları kullanmakta ve riskleri en aza indirmek için istenmeyen posta önleme filtrelerinden yararlanmaktadır.

8.4.1. E-posta Tarayıcısı Prensipleri

E-posta Tarayıcısı bileşeni gelen/giden e-postaları otomatik olarak tarar. Bunu, AVG'de kendi eklentisi olmayan e-posta istemcileriyle kullanabilirsiniz (örn. Outlook Express, Mozilla, Incredimail vb.).

AVG [yüklemesi sırasında](#) AVG e-posta kontrolü için oluşturulmuş otomatik sunucular bulunur: biri gelen e-postaları kontrol etmek ve ikincisi giden e-postaları kontrol etmek için. Bu iki sunucu kullanılarak e-postalar otomatik olarak 110 ve 25 bağlantı noktalarında (*e-posta göndermek/alma için standart bağlantı noktaları*) kontrol edilir.

E-Posta Tarayıcısı İnternet'te e-posta istemcisi ve e-posta sunucuları arasında arayüz olarak çalışır.

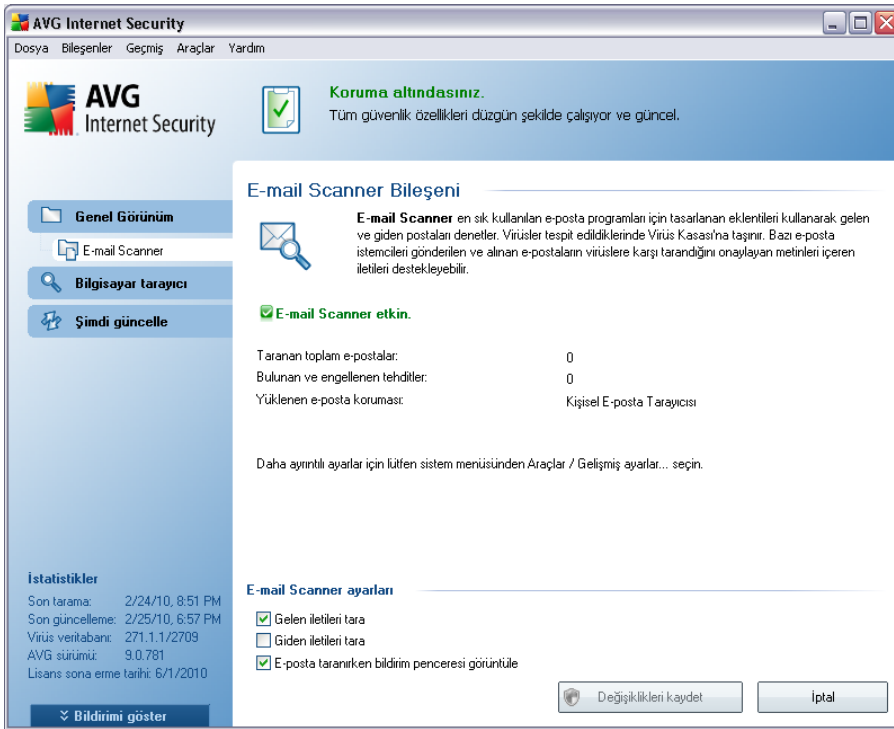
- **Gelen posta:** Sunucudan bir ileti alırken, **E-posta Tarayıcısı** bileşeni bunun

virüs içerip içermediğini kontrol eder, virüslü ekleri kaldırır ve sertifika ekler. Tespit edildikleri zaman virüsler anında **Virüs Kasasında** karantina altına alınacaktır. Ardından ileti, e-posta istemcisine aktarılır.

- **Giden posta:** İleti e-posta istemcisinden E-posta Tarayicisine gönderilir; o da iletiyi ve eklerinin virüslü olup olmadığını kontrol eder ve sonra mesajı SMTP sunucuna gönderir (*giden e-postaları tarama varsayılan olarak devre disidir ve elle ayarlanabilir*).

Not: AVG E-posta Tarayicisinin sunucu platformlarında kullanılması hedeflenmemiştir!

8.4.2. E-posta Tarayicısı Arayüzü



E-Posta Tarayicisi bileşeninin iletişim kutusunda bileşenlerin fonksiyonlarını, mevcut durumu hakkında bilgiyi (*E-Posta Tarayicisi bileşeni aktiftir.*) ve aşağıdaki istatistikleri bulabilirsiniz:

- **Taranan toplam e-posta sayısı - E-posta Tarayicisi** son çalıştırıldığından beri kaç adet e-postanın tarandığı hakkında bilgi verir (*gerekliyse bu değer sıfırlanabilir; Örn. istatistiki amaçlar için - Degeri Sifirla*)

- **Bulunan ve engellenen tehditler - E-posta Tarayicisi** son alistirildigindan beri e-posta mesajlari iinde tespit edilen bulasmalarin sayisi hakkında bilgi verir
- **Yüklü e-posta koruma** - Varsayilan ve yüklü e-posta istemcisine iliskin belirli bir e-posta koruma eklentisi hakkında bilgi verir

Temel bileşen yapılandırma

İletişim kutusunun alt kısmında bileşenin fonksiyonlarının ana özelliklerinden bazılarını düzenleyebileceğiniz **E-posta Tarayicisi ayarları** adı altında bir bölüm bulunmaktadır.

- **Gelen iletileri tara** - Hesabınıza teslim edilen tüm e-postalarda virüs taraması yapılması için bu öğeyi işaretleyin. Varsayilan olarak, bu öğe açıktır ve bu ayarı deęistirmemeniz önerilir!
- **Giden mesajları tara** - Hesabınızdan gönderilen tüm e-postaların virüslere karşı taranmasını onaylamak için öğeyi işaretleyin. Varsayilan olarak bu öğe kapalıdır.
- **E-posta taranırken bildirim simgesini görüntüle** - Postanız [E-mail Scanner](#) bileşeni ile taranırken sistem tepsisinde AVG simgesi üzerinde görüntülenen bildirim iletişim kutusu yoluyla bilgilendirilmek istediğinizi onaylamak için öğeyi işaretleyin. Varsayilan olarak, bu öğe açıktır ve bu ayarı deęistirmemeniz önerilir!

E-posta Tarayicisi bileşeninin gelişmiş konfigürasyonuna **Aralar/Gelişmiş ayarlar** ögesinden ulaşabilirsiniz ancak gelişmiş yapılandırmanın sadece uzman kullanıcılar tarafından gerçekleştirilmesi önerilmektedir!

Lütfen dikkat: Yazılım satıcısı, en iyi performansın sunulabilmesi için tüm AVG bileşenlerini kurmuştur. Bunun için iyi bir nedeniniz olmadıka AVG yapılandırmasını deęistirmeyin. Ayarlarda yapılacak her tür deęisiklik sadece deneyimli bir kullanıcı tarafından gerçekleştirilmelidir. AVG yapılandırmasını deęistirmeniz gerekiyorsa sistem menüsünden ilgili öğeyi seçin **Aralar/Gelişmiş ayarlar** ve yeni açılan [AVG Gelişmiş Ayarlar](#) iletişim kutusunda AVG yapılandırmasını düzenleyin.

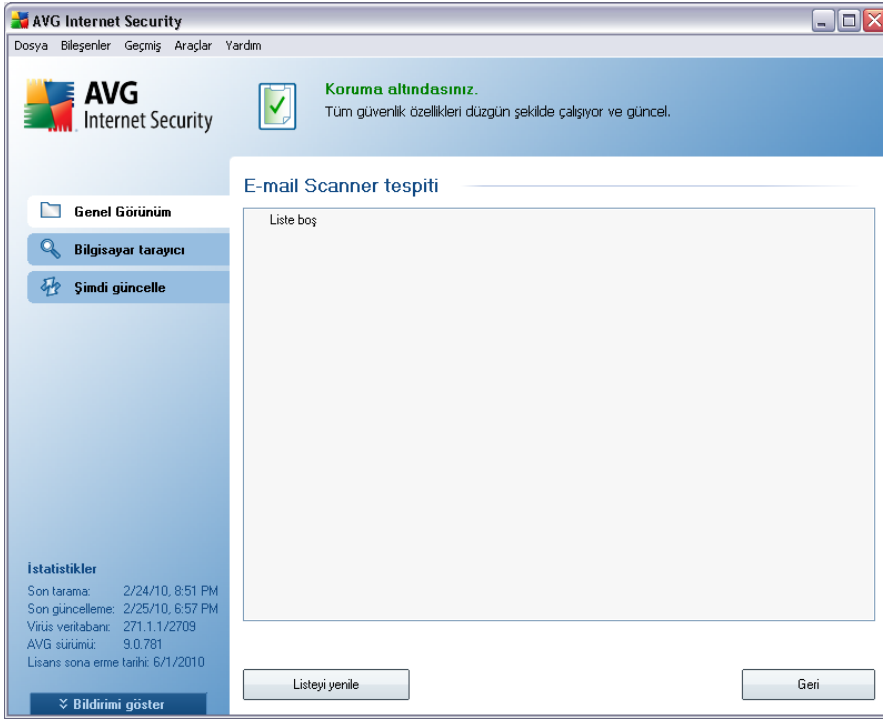
Kontrol düğmeleri

E-posta Tarayicisi arayüzünde bulunan kontrol düğmeleri şunlardır:

- **Deęisiklikleri kaydet** bu iletişim kutusunda yapılan her tür deęisiklięi kaydetmek ve uygulamak için bu düğmeye basın

- ***Iptal*** - Varsayılan [AVG kullanıcı arayüzüne](#) dönmek için bu düğmeye basın (bileşenlere genel bakış)

8.4.3. E-posta Tarayıcısı Tespiti



E-Posta Tarayıcısı Tespiti iletişim kutusunda (*sistem menüsü seçeneği Geçmiş / E-Posta Tarayıcısı Tespiti üzerinden erişebilirsiniz*) ***E-Posta Tarayıcısı*** bileşeni tarafından tespit edilen tüm bulguların bir listesini görebilirsiniz. Tespit edilen tüm nesneler için aşağıdaki bilgiler verilir:

- ***Bulasma*** - Algılanan nesnenin açıklaması (Muhtemelen adı da)
- ***Nesne*** - nesnenin konumu
- ***Sonuç*** - tespit edilen nesne ile gerçekleştirilen eylem
- ***Algılama zamanı*** - Şüpheli nesnenin algılandığı tarih ve saat
- ***Nesne Türü*** - tespit edilen nesnenin türü

İletişim kutusunun alt kısmında, listenin altında yukarıda listelenen tespit edilen

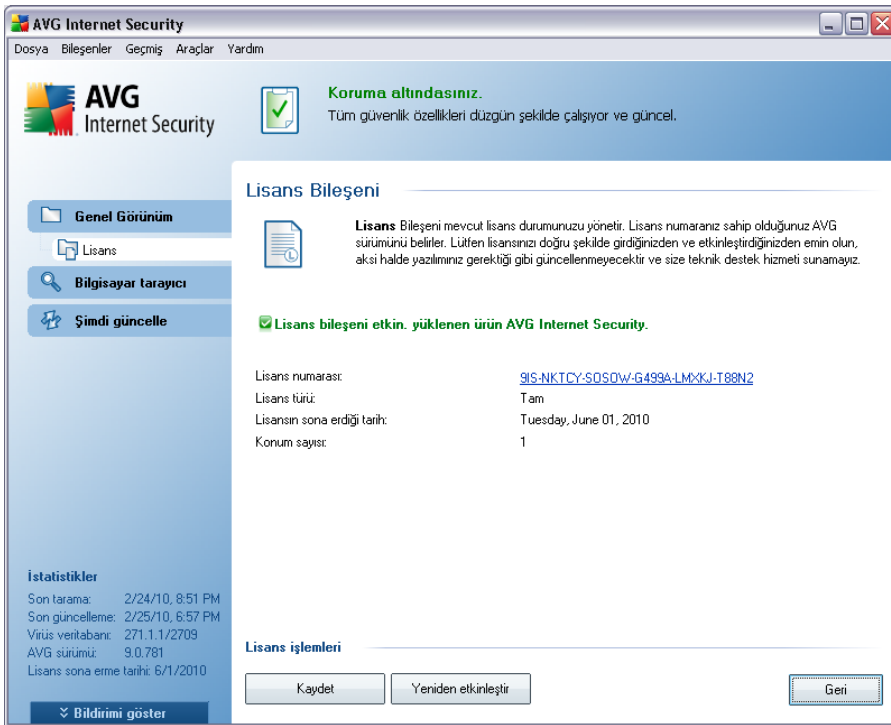
nesnelerin toplam sayisi hakkında bilgi bulabilirsiniz. Buna ek olarak tespit edilen nesneler listesini ayrı bir dosyada dışa aktarabilir (**Listeyi Dosyaya Aktar**) ve tespit edilen nesneler hakkındaki tüm girişleri silebilirsiniz (**Listeyi Temizle**).

Kontrol düğmeleri

E-posta Tarayicisi algilama arayüzünde bulunan kontrol düğmeleri şunlardır:

- **Listeyi yenile** - Algılanan tehlikelerin listesini günceller
- **Geri** - Sizi varsayılan [AVG kullanıcı arayüzüne](#) (bilesenlere genel bakış) geri döndürür

8.5. Lisans



Lisans bileşeninin iletişim kutusunda, bileşenlerin fonksiyonlarını, mevcut durumu hakkında bilgiyi (*Istenmeyen Posta Önleme bileşeni aktiftir.*), ve aşağıdaki bilgileri bulabilirsiniz:

- **Lisans numarası** - lisans numaranızın mevcut durumunu gösterir. Lisans numaranızı girerken çok dikkatli olmalı ve gösterildiği gibi girmelisiniz. Bu yüzden, lisans numarasıyla ilgili bir düzeltme için her zaman "kopyala ve yapıştır" yöntemini kullanmanızı önemle öneririz.
- **Lisans türü** - Yüklenen ürün türünü belirtir.
- **Lisans sonu** - bu tarih, lisans numaranızın geçerlilik süresini belirler. Bu tarihten sonra **AVG 9 Anti-Virus** programını kullanmaya devam etmek istiyorsanız lisansınızı yenilemeniz gerekir. [Lisans yenileme](http://www.avg.com/) AVG web sitesinden (<http://www.avg.com/>) çevrimiçi gerçekleştirilebilir.
- **Kullanıcı sayısı** - **AVG 9 Anti-Virus** programınızı yükleme hakkınız olan çalışma istasyonu sayısıdır.

Kontrol düğmeleri

- **Kaydol** - AVG web sitesi (<http://www.avg.com/>) kayıt sayfasına bağlanır. Lütfen kayıt bilgilerinizi doldurun; sadece AVG ürünlerini kaydettiren müşterilerimiz ücretsiz teknik destek alabilecektir.
 - **Yeniden Etkinleştir** - **yükleme işleminin** AVG'yi Kisiselleştir [iletisim kutusuna girilen verilerle](#) AVG'yi Etkinleştir [iletisim kutusunu açar](#). Bu iletisim kutusunda satış numaranızı (AVG'yi yüklerken kullandığınız numara), ya da eski lisans numaranızı (Örn. yeni bir AVG ürününe geçerken) değiştirmek için lisans numaranızı girebilirsiniz.
- Not:** AVG 9 Anti-Virus **deneme sürümünü kullanıyorsanız, düğmeler Simdi satın al ve Etkinleştir** olarak görünür, programın tam sürümünü hemen satın almanızı sağlar. Bir satış numarasıyla yüklenmiş **AVG 9 Anti-Virus** için, düğmeler **Kaydet** ve **Etkinleştir** olarak görünür.
- **Geri** - Varsayılan [AVG kullanıcı arayüzüne](#) dönmek için bu düğmeye basın (bileşenlere genel bakış).

8.6. Bağlantı Tarayıcı

8.6.1. Link Scanner Prensipleri

LinkScanner bileseni, web tarayicisi ya da eklentileri yoluyla bilgisayarınıza kötü amaçlı yazılım yüklemek için tasarlanmış web sitelerine karşı koruma sağlar. **LinkScanner** teknolojisi iki özellik içerir, [AVG Search-Shield](#) ve [AVG Active Surf-Shield](#):

- [AVG Search Shield](#) tehlikeli olduğu bilinen web sitelerinin listesini (URL adresleri) içerir. Google, Yahoo!, Bing, Baidu, Altavista veya Yandex'te arama yaparken, aramanın tüm sonuçları bu listeye göre kontrol edilir ve bir karar simgesi gösterilir (Yahoo! arama sonuçları için yalnızca "yararlanılan web sitesi" karar simgeleri gösterilir) gösterilir. Bunun yanı sıra doğrudan tarayicinize girdiğiniz adresler, web sitelerinde ya da e-postanızdan tıkladığınız diğer bağlantılar da otomatik olarak kontrol edilir ve gerekli olması halinde engellenir.
- [AVG Active Surf-Shield](#) web sitesinin adresi önemli olmaksızın ziyaret etmekte olduğunuz web sitelerinin içeriklerini tarar. Web sitesi [AVG Search Shield](#) (örn. yeni bir zararlı web sitesi oluşturulduğunda veya önceden temiz olan bir web sitesi artık kötü amaçlı yazılım içerdiğinde) tarafından algılanmasa da ziyaret etmeye çalıştığınızda [AVG Active Surf-Shield](#) tarafından algılanıp engellenir.

Not: AVG LinkScanner'ın sunucu platformlarında kullanılması hedeflenmemiştir!

8.6.2. Link Scanner Arayüzü

LinkScanner bileseni, **LinkScanner** bileseninin arayüzünden açıp kapatabileceğiniz iki bölümden oluşur:

LinkScanner bileseni arayüzü bilesenlerin işlevselliği hakkında kısa açıklama ve geçerli durum hakkında bilgi sağlar (*LinkScanner bileseni etkin.*). Ayrıca, en güncel **LinkScanner** veritabanı sürüm numarası (*LinkScanner Sürümü*) hakkında bilgi bulabilirsiniz.



İletişim kutusunun en alt bölümünde birçok seçeneği düzenleyebilirsiniz:

- **AVG Search-Shield'i** Etkinleştir - (*varsayılan olarak açıktır*): arama motorunca getirilen sitelerin içeriğinin önceden kontrol edildiğine dair Google, Yahoo!, Bing, Baidu, Yandex, veya Altavista'da yapılan aramalara ilişkin bilgilendirici simgeler.
- **AVG Active Surf-Shield'i etkinleştir** - (*varsayılan olarak açıktır*): erişim sağlandığı anda güvenlik açığı olan web sitelerine karşı koruma (*gerçek zamanlı*) sağlamak için etkinleştirin. Bilinen zararlı site bağlantıları ve zararlı içerikleri, kullanıcı tarafından bir web tarayıcısı (ya da HTTP kullanan diğer bir program) üzerinden erişim sağlandığı anda engellenir.
- **Algılanan tehlikelerin AVG'ye rapor edilmesini etkinleştir** - Web'deki zararlı etkinlikler hakkında bilgi toplayan veritabanına bilgi sağlamak için **Güvenli Gezinme** ya da **Güvenli Arama** tarafından tespit edilen güvenlik açıklarının ve kötü sitelerin rapor edilmesini istiyorsanız bu öğeyi işaretleyin.

8.6.3. AVG Arama Kalkanı

AVG Search-Shield açık durumdayken Internet'te dolasırken Yahoo!, Google, Bing, Altavista, Yandex vb. yaygın tarama motorlarından gelen tüm sonuçlar tehlikeli veya şüpheli bağlantılar yönünden değerlendirilir. Bu bağlantıları kontrol ederek ve kötü bağlantıları isaretleyerek, **AVG Link Scanner** sizi tehlikeli veya şüpheli bağlantıları tıklatmadan önce uyarır, böylece yalnızca güvenli web sitelerine gittiginizden emin olursunuz.

Arama sonuçları sayfasında bağlantı değerlendirilirken bağlantının yanında bağlantı teyidi işleminin devam etmekte olduğunu gösteren bir grafik isareti görürsünüz. Değerlendirme işlemi tamamlandığında, ilgili bilgilendirme simgesi görüntülenir:

 Bağlantı verilen sayfa güvenli. (Yahoo! arama motoru ile [AVG Security Toolbar](#) bu simge gösterilmeyecektir!).

 }Bağlantılı sayfa tehlike içermiyor, ancak bazı şeyler şüpheli (orijin ve davranış olarak şüpheli olduğundan e-alisveris vb. için önerilmez.).

 Bağlantılı sayfa güvenli olabilir, ancak şu anda doğrudan herhangi bir tehlike bulunmasa bile tehlikeli ya da kod olarak şüpheli olabilecek sayfalara bağlantılar içermekte.

 Bağlantı verilen sayfa etkin tehlike içeriyor! Kendi güvenliğinizi için, bu sayfayı ziyaret etmenize izin verilmeyecek.

 Bağlantılı sayfaya erişilemediğinden taranamadı.

Tek tek değerlendirme simgesinin üzerine gelindiğinde, sorgulanan belirli bağlantıyla ilgili bilgiler gösterilir. Tehditle (varsa) ilgili ek bilgiler, bağlantı IP adresi ve sayfanın AVG tarafından ne zaman tarandığı gibi bilgiler:



Güvenli: Bu sayfa aktif tehlike içermiyor.

Açıklama:
Bu sayfaya devam etmek güvenli.
IP Adresi: 221.236.206.3
Tarama süresi: 02/25/10 19:16:35
(0.09 bu sayfayı taramak için saniye cinsinden süre)
Derecelendirmeler AVG tarafından sağlanmıştır. Site sahipleri, sorularınız için lütfen AVG ile irtibata geçin.

En son AVG haberleri ve güncellemeleriyle
güncel tutun. AVG web sitesini ziyaret edin.

[burayı tıklayın](#)

8.6.4. AVG Aktif Gezinme Kalkanı

Bu güçlü koruma, açmaya çalıştığınız web sayfalarının kötü amaçlı içeriğini engeller ve bilgisayarınıza karsidan yüklenmesini önler. Bu özellik etkin durumdayken, tehlikeli bir site bağlantısı tıklatıldığında ya da URL'si yazıldığında otomatik olarak web sayfasını açmanız engellenir, bu sayede etkilenmeniz önlenmiş olur. Etkilenen siteyi ziyaret ederek güvenlik açıkları olan web sayfalarının bilgisayarınızı kolaylıkla etkileyebileceğini unutmamak önemlidir, bu nedenle açıklardan yararlanma veya diğer ciddi tehlikeler içeren tehlikeli bir web sayfası isteginde bulunduğunuzda, [AVG Link Scanner](#), tarayıcınızın bu sayfayı göstermesine izin vermez.

Kötü amaçlı bir web sitesiyle karsilasirsaniz, [AVG Link Scanner](#) sizi suna benzer bir ekranla uyaracaktır:



Bu tür bir web sitesine girmek oldukça risklidir ve önerilemez!

8.7. Çevrimiçi Kalkan

8.7.1. Online Shield İlkeleri

Online Shield ziyaret ettiğiniz web sitelerinin içeriğini (muhtemel dosyalar dahil olmak üzere), henüz web tarayıcınızda görünmeden ya da bilgisayarınıza indirilmeden önce tarayan gerçek zamanlı bir koruma yöntemidir.

Online Shield, ziyaret ettiğiniz sayfanın tehlikeli javascript içerdiğini tespit ederse, sayfanın görüntülenmesini engeller. Buna ek olarak bir sayfada bulunan zararlı yazılımı tanır ve bilgisayarınıza girişini engellemek için indirme işlemini durdurur.

Not: AVG Online Shield'in sunucu platformlarında kullanılması hedeflenmemiştir!

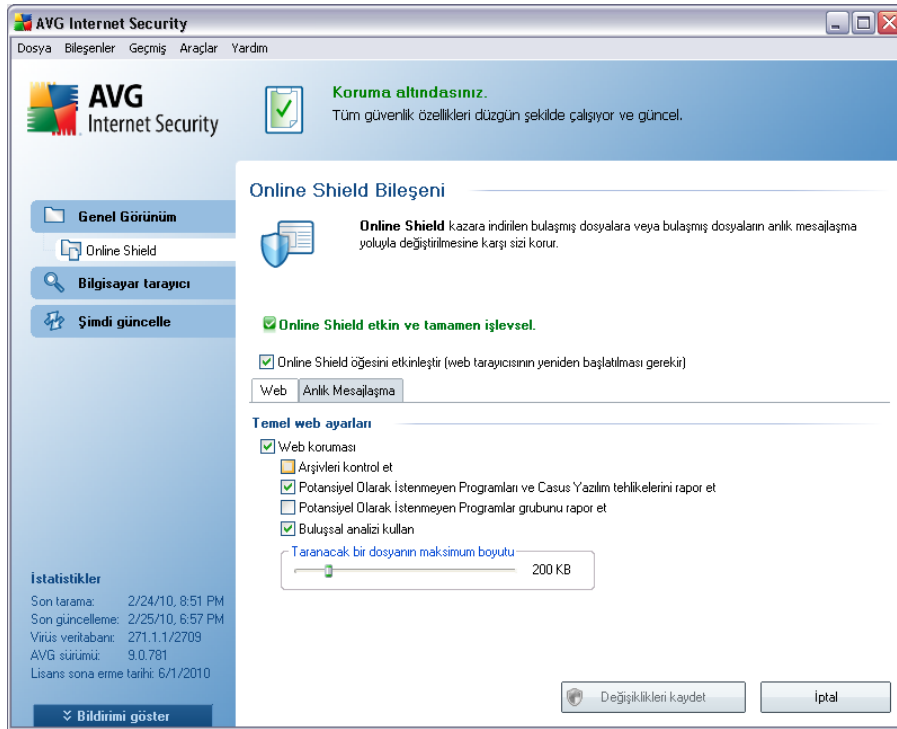
8.7.2. Online Shield Arayüzü

Online Shield bileşeninin arayüzünde, bu tür koruma tipinin davranışı tanımlanır. Buna ek olarak bileşenin mevcut durumu hakkında bilgi de elde edebilirsiniz (*Online Shield* aktiftir ve tamamen işlevseldir.). İletişim penceresinin alt kısmında bileşenin fonksiyonlarının düzenlenmesi açısından kullanılan basitçe seçenekler bulunmaktadır.

Temel bileşen yapılandırma

İlk olarak **Online Shield'i Etkinleştir** ögesini seçerek ya da seçmeyerek **Online Shield'i** istediğiniz zaman açıp kapatabilirsiniz. Bu seçenek varsayılan olarak etkin ve **Online Shield** bileşeni aktiftir. Diğer bir yandan, bu ayarları değiştirmek açısından geçerli bir nedeniniz yoksa bileşeni devre dışı bırakmamanızı öneririz. Bu öğe işaretliken **Online Shield** çalışır; iki sekme üzerinde daha fazla yapılandırma seçeneği bulunmaktadır ve düzenlenebilirler:

- **Web** - web sitelerinin içeriğinin taranmasına ilişkin bileşen yapılandırmasını düzenleyebilirsiniz. Düzenleme arayüzü ile aşağıdaki temel seçenekleri yapılandırabilirsiniz:



- o **Web koruması** - bu seçenek **Online Shield**'in www sayfalarının içeriğini taraması gerektiğini onaylar. Bu seçeneğin etkin konumda olmasına rağmen (*varsayılan olarak*) söz konusu öğeleri açıp kapatabilirsiniz:
 - **Arsivleri kontrol et** - görüntülenecek www sayfasında bulunan arşivlerin içeriğini tarar
 - **Potansiyel Olarak İstenmeyen Programları ve Casus Yazılım tehlikelerini rapor et** - (*varsayılan olarak açıktır*): [Anti-Spyware](#) motorunu etkinleştirmek ve virüslerle birlikte casus yazılımları da kontrol etmek için işaretleyin. [Casus yazılım](#), kötü amaçlı yazılım olabilecek kategorisini temsil eder: bir güvenlik riski oluştursa da bu programlardan bazıları bilerek yüklenebilir. Bilgisayarınızın güvenliğini artırdığından, bu özelliği etkin durumda tutmanızı öneriyoruz
 - **Gelismiş Potansiyel Olarak İstenmeyen Programlar setini bildir** - önceki seçenek etkinleştirilirse, genişletilmiş [casus yazılım](#) paketini algılamak için bu kutuyu da işaretleyebilirsiniz: doğrudan üreticiden alınan tamamen zararsız olan, ancak daha sonra kötüye kullanılan programlar. Bu, bilgisayar güvenliğinizi daha da artıran ek bir önlemdir, ancak yasal programları da engelleyebilir ve bu yüzden varsayılan olarak kapalıdır.
 - **Bulussal analizi kullan** - bulussal analiz yöntemiyle görüntülenecek sayfanın içeriğini tarar, örn. sanal bilgisayar ortamında taranan nesnenin talimatlarının simülasyonu ve değerlendirilmesi. Bu nedenle, virüs veritabanında henüz açıklanmayan zararlı kodları bile tespit edebilir. (bkz. [Anti-Virüs İlkeleri](#)).
 - **Taranacak maksimum dosya büyüklüğü** - dahil edilen dosyalar görüntülenen sayfada mevcutsa, bunları bilgisayarınıza indirmeden önce de içeriklerini tarayabilirsiniz. Ancak büyük dosyaların taranması zaman alabilir ve web sayfasının indirilmesi de önemli ölçüde yavaşlayabilir. **Online Shield** ile taranacak dosyanın maksimum boyutunu belirlemek için kaydırma çubuğunu kullanabilirsiniz. İndirilen dosya belirtilen dosya boyutundan daha büyük olsa ve buna bağlı olarak Online Shield ile taranmasa bile korunmaya devam edersiniz: dosyaya virüs bulamış olması halinde **Yerlesik Kalkan*** tarafından hemen tespit edilecektir**.
- **Anlık Mesajlaşma** - anlık mesajlaşma (Örn. ICQ, MSN Messenger, Yahoo ...) taramasına ilişkin bileşen ayarlarını yapılandırabilmenizi sağlar.



- o Anlık Mesajlaşma koruması - Online Shield'in çevrimiçi iletişimin virüsten etkilenmediğini belirlemesini istiyorsanız bu öğeyi işaretleyin. Bu seçeneğin etkin olması kaydıyla ayarlarınızı, kontrol etmek istediğiniz anlık mesajlaşma uygulamasına uygun olacak şekilde yapılandırabilirsiniz- su an sadece **AVG 9 Anti-Virus** ICQ, MSN, ve Yahoo uygulamaları desteklenmektedir.

Lütfen dikkat: Yazılım satıcısı, en iyi performansın sunulabilmesi için tüm AVG bileşenlerini kurmuştur. Bunun için iyi bir nedeniniz olmadıkça AVG yapılandırmasını değiştirmeyin. Ayarlarda yapılacak her tür değişiklik sadece deneyimli bir kullanıcı tarafından gerçekleştirilmelidir. AVG yapılandırmasını değiştirmeniz gerekiyorsa sistem menüsünden ilgili öğeyi seçin **Araçlar/Gelişmiş ayarlar** ve yeni açılan [AVG Gelişmiş Ayarlar](#) iletişim kutusunda AVG yapılandırmasını düzenleyin.

Kontrol düğmeleri

Online Shield arayüzünde bulunan kontrol düğmeleri şunlardır:

- **Değişiklikleri kaydet** bu iletişim kutusunda yapılan her tür değişikliği kaydetmek ve uygulamak için bu düğmeye basın

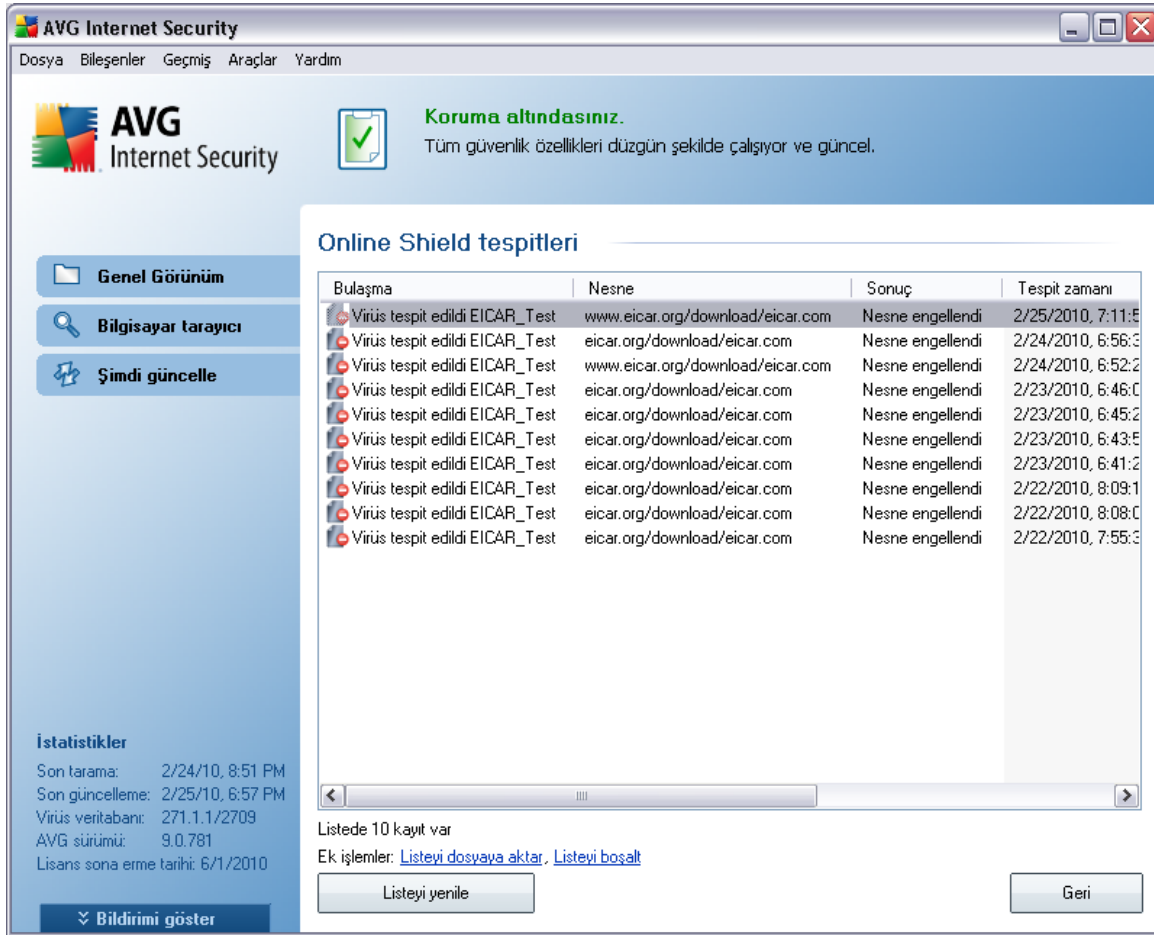
- **Iptal** - Varsayılan [AVG kullanıcı arayüzüne](#) dönmek için bu düğmeye basın (bileşenlere genel bakış)

8.7.3. Online Shield Algılaması

Online Shield ziyaret ettiğiniz web sitelerinin içeriklerini ve sitelerin içindeki muhtemel dosyaları, ilgili web sitesi henüz tarayicinizda görünmeden ya da bilgisayarınıza indirmeden tarar. Bir tehdit tespit edilirse aşağıdaki iletişim kutusu vasıtasıyla hemen uyarılırsınız:



Süpheli web sayfası açılmayacaktır ve tehlike algılama **Online Shield bulguları** listesi günlüğüne alınacaktır - algılanan tehlikelere bu genel bakışa sistem menüsünün [Geçmiş / Web Shield Tespitleri](#) ögesinden erişilebilir.



Tespit edilen tüm nesneler için aşağıdaki bilgiler verilir:

- **Bulaşma**- Algılanan nesnenin açıklaması (*Muhtemelen adi da*)
- **Nesne** - Nesne kaynağı (*web sayfası*)
- **Sonuç** - tespit edilen nesne ile gerçekleştirilen eylem
- **Algılama zamanı** - Tehlikenin algılandığı ve engellendiği tarih ve saat
- **Nesne Türü** - tespit edilen nesnenin türü
- **İşlem** -tespit edilmesi amacıyla potansiyel tehlike taşıyan nesneyi uyarın işlem nedir

İletişim kutusunun alt kısmında, listenin altında yukarıda listelenen tespit edilen nesnelerin toplam sayısı hakkında bilgi bulabilirsiniz. Buna ek olarak tespit edilen nesneler listesini ayrı bir dosyada dışa aktarabilir (**Listeyi Dosyaya Aktar**) ve tespit edilen nesneler hakkındaki tüm girişleri silebilirsiniz (**Listeyi Temizle**). **Listeyi yenile** düğmesi, **Online Shield** tarafından algılanan bulgular listesini günceller. **Geridüğmesi**, sizi varsayılan [AVG kullanıcı arayüzüne](#) götürür (bilesenlere genel bakış).

8.8. Yerleşik Kalkan

8.8.1. Yerleşik Kalkan Prensipleri

Yerlesik Kalkan bileseni, bilgisayarınızın sürekli olarak korunmasını sağlar. Açılan, kaydedilen veya kopyalanan her dosyayı tarar ve bilgisayarın sistem alanlarını korur. **Yerlesik Kalkan** erişilen bir dosyada virüs tespit ederse geçerli işlemi durdurur ve virüsün kendisini etkinleştirmesine izin vermez. Normal olarak, "arka planda" çalıştığından işlemi fark etmezsiniz ve yalnızca tehdit bulunması durumunda bilgilendirilirsiniz; aynı anda, **Yerlesik Kalkan** tehdidin etkinleştirilmesini engeller ve tehdidi kaldırır. **Yerlesik Kalkan** sistemin başlatılması sırasında bilgisayarınızın belleğine yüklenir.

Uyarı: Yerlesik Kalkan, başlatma sırasında bilgisayarınızın belleğine yüklenir ve bu özelliği her zaman açık durumda tutmanız önemlidir!

8.8.2. Yerleşik Kalkan Arayüzü



En önemli istatistiki verilerin ve bileşenin mevcut durumu hakkındaki bilgilerin yanı sıra (*Yerleşik Kalkan* aktiftir ve tamamen fonksiyoneldir) **Yerleşik Kalkan** arayüzü, bileşenin ayarlarına dair bazı seçenekler de sunar. İstatistikler aşağıdaki gibidir:

- **Yerleşik Kalkan** 'den beri etkin - bileşenin en son çalıştırıldığı tarihten itibaren geçen zamanı gösterir
- **Tespit edilen ve engellenen tehditler** - çalıştırılması/açılması engellenen tespit edilen bulasma sayısı (*ihtiyaç duyulursa bu değer sıfırlanabilir; Örn. istatistiki amaçlar doğrultusunda - Değeri sıfırla*)

Temel bileşenin yapılandırma

İletişim penceresinin alt kısmında **Yerleşik Kalkan ayarları** adı altında bir bölüm göreceksiniz; burada bileşenin fonksiyonlarının temel ayarlarından bazılarını düzenleyebilirsiniz (*diğer bileşenlerde de olduğu gibi ayrıntılı yapılandırma, sistem menüsünün Araçlar/Gelişmiş ayarlar ögesinden yapılabilmektedir*).

Yerlesik Kalkan Etkin seçeneği yerlesik korumayı kolaylıkla açıp kapatabilmenizi sağlar. Varsayılan olarak bu fonksiyon açıktır. Yerlesik koruma açık durumdayken tespit edilen bulasmalar hususunda gerçekleştirilecek eylemi (silmeyi) belirleyebilirsiniz:

- o otomatik olarak (**Tüm tehditleri otomatik olarak sil**)
- o ya da sadece kullanıcının onayının ardından (**Tehditleri silmeden önce bana sor**)

Bu seçimin güvenlik seviyesi üzerinde herhangi bir etkisi yoktur ve sadece tercihlerinizi yansıtır.

Her iki durumda da **İzleme tanımlama bilgilerini tara** işlemini yapmayı veya yapmamayı seçebilirsiniz. Belirli durumlarda maksimum güvenlik seviyesine ulaşmak için bu seçeneği kullanabilirsiniz fakat varsayılan olarak kapalıdır. (*tanımlama bilgileri = bir sunucu tarafından web tarayıcısına ve oradan da siteye her ulaşıldığında değiştirilmeksizin tarayıcı tarafından geri gönderilen metin parçalarıdır. HTTP tanımlama bilgileri, site tercihleri veya elektronik alışveriş sepetlerinin içerikleri gibi kullanıcılar hakkındaki belirli bilgilerin kimliklerinin doğrulanması, takibi ve sürdürülmesi için kullanılır.*)

Lütfen dikkat: Yazılım satıcısı, en iyi performansın sunulabilmesi için tüm AVG bileşenlerini kurmuştur. Bunun için iyi bir nedeniniz olmadıkça AVG yapılandırmasını değiştirmeyin. Ayarlarda yapılacak her tür değişiklik sadece deneyimli bir kullanıcı tarafından gerçekleştirilmelidir. AVG yapılandırmasını değiştirmeniz gerekiyorsa sistem menüsünden ilgili öğeyi seçin **Araçlar/Gelişmiş ayarlar** ve yeni açılan [AVG Gelişmiş Ayarlar](#) iletişim kutusunda AVG yapılandırmasını düzenleyin.

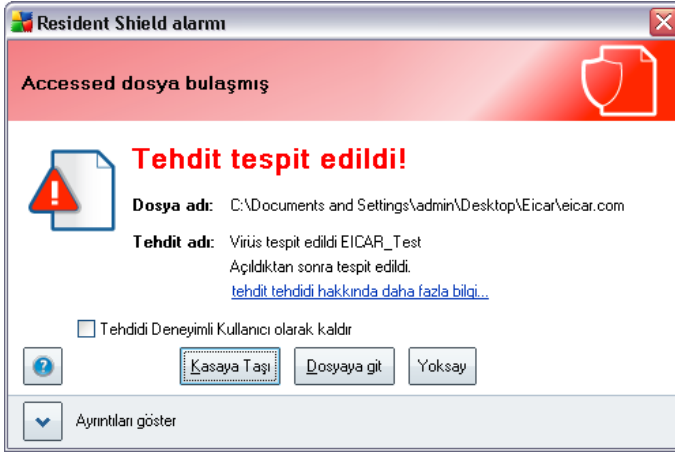
Kontrol düğmeleri

Yerlesik Kalkan arayüzünde bulunan kontrol düğmeleri şunlardır:

- **İstisnaları yönet-** [Yerlesik Kalkan](#) taraması dışında tutulacak klasörleri tanımlayabileceğiniz [Yerlesik Kalkan - Dizin Disi Birakılanlar](#) iletişim kutusunu açar.
- **Değişiklikleri kaydet** bu iletişim kutusunda yapılan her tür değişikliği kaydetmek ve uygulamak için bu düğmeye basın
- **İptal** - Varsayılan [AVG kullanıcı arayüzüne](#) dönmek için bu düğmeye basın (bileşenlere genel bakış)

8.8.3. Yerleşik Kalkan Tespiti

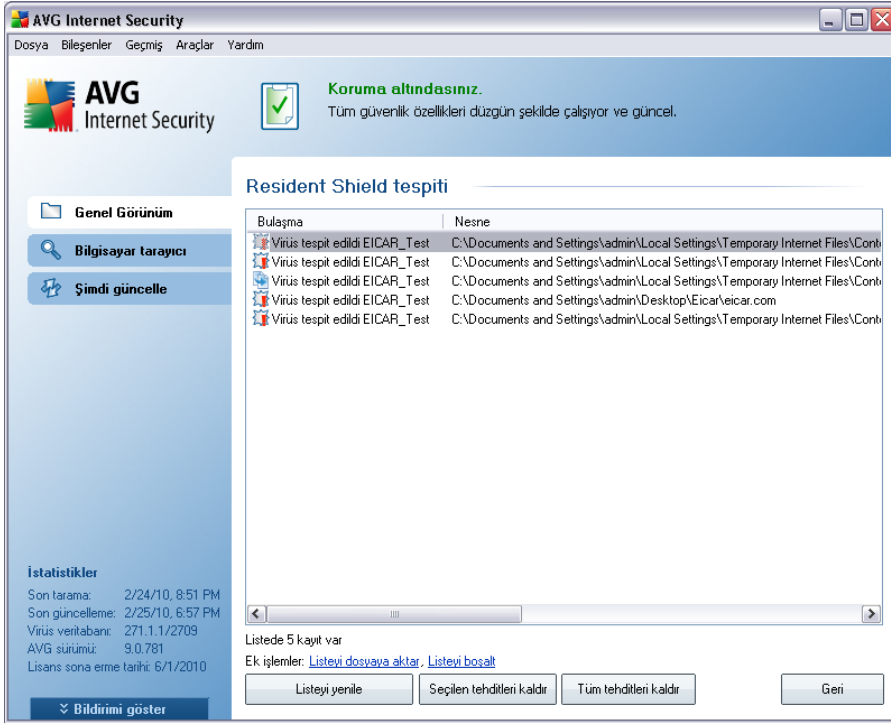
Yerleşik Kalkan dosyalar kopyalanırken, açılırken ya da kaydedilirken söz konusu dosyaları tarar. Herhangi bir virüs ya da bir tehdit tespit edildiği zaman aşağıdaki iletişim kutusu ile anında uyarılırsınız:



İletişim kutusunda tespit edilen tehdit hakkında bilgi bulunmakta ve sizden hangi eylemin yapılmasını istediğinizi belirtmeniz istenmektedir:

- **Temizle** - Temizleme yöntemi mevcut ise AVG, bulaşan nesneyi otomatik olarak temizleyecektir, bu seçenek ilk olarak seçilmesi gereken eylemlerdendir.
- **Kasaya Tasi** - Virüs AVG [Virüs Kasasına tasınacaktır](#)
- **Dosyaya git** - Bu seçenek sizi şüpheli nesnenin tam konumuna yönlendirir (*yeni Windows Gezgini penceresi açar*)
- **Gözardi Et** - çok geçerli bir nedeninizin olmaması halinde KESİNLİKLE bu seçeneği seçmemenizi öneriyoruz!

[Yerleşik Kalkan](#) tarafından algılanan tüm tehlikelerin tamamına genel bakış **Yerleşik Kalkan algılama** iletişim kutusunda bulunabilir, buna [Geçmiş / Yerleşik Kalkan bulguları](#) sistem menüsü seçeneğinden erişebilirsiniz:



Yerlesik Kalkan tespiti Yerlesik Kalkan tarafından tespit edilip tehlikeli olduğu görülen ve temizlenen ya da Virüs Kasasına tasınan nesneler hakkında genel bilgi vermektedir. Tespit edilen tüm nesneler için aşağıdaki bilgiler verilir:

- **Bulasma**- Algılanan nesnenin açıklaması (Muhtemelen adı da)
- **Nesne** - nesnenin konumu
- **Sonuç** - tespit edilen nesne ile gerçekleştirilen eylem
- **Algılama zamanı** - Nesnenin algılandığı tarih ve saat
- **Nesne Türü** - tespit edilen nesnenin türü
- **İslem** -tespit edilmesi amacıyla potansiyel tehlike taşıyan nesneyi uyarın işlem nedir

İletişim kutusunun alt kısmında, listenin altında yukarıda listelenen tespit edilen nesnelerin toplam sayısı hakkında bilgi bulabilirsiniz. Buna ek olarak tespit edilen nesneler listesini ayrı bir dosyada dışa aktarabilirsiniz (**Listeyi Dosyaya Aktar**) ve tespit edilen nesneler hakkındaki tüm girişleri silebilirsiniz (**Listeyi Temizle**). **Listeyi Yenile**

düğmesi, **Yerlesik Kalkan** tarafından tespit edilen buluntular listesini günceller. **Geri** düğmesi, sizi varsayılan [AVG kullanıcı arayüzüne](#) götürür (bilesenlere genel bakış).

8.9. Güncelleme Yöneticisi

8.9.1. Güncelleme Yöneticisi Prensipleri

Güvenlik yazılımlarının hiçbirisi, rutin olarak güncellenmediği takdirde sizi çeşitli tehditlere karşı korumayı garanti edemez! Virüs yazarları, yazılım ve işletim sistemlerinde yararlanabilecekleri güvenlik açıkları aramaktadır. Her gün yeni virüsler, yeni zararlı yazılımlar ve yeni bilgisayar saldırıları gerçekleştirilmektedir. Bu nedenle yazılım geliştiricileri, tespit edilen güvenlik açıklarını kapatmak üzere devamlı olarak güncellemeler ve güvenlik paketleri yayınlamaktadır.

AVG'nizi rutin olarak güncellemeniz çok önemlidir!

Güncelleme Yöneticisi rutin güncelleme işlemini kontrol etmenize yardımcı olur. Bu bileşen kapsamında, güncelleme dosyalarını İnternet'ten ya da yerel ağdan otomatik olarak indirmeyi seçebilirsiniz. Gerekli virüs tanımlı güncellemelerinin mümkün ise her gün yapılması gerekmektedir. Daha az önem taşıyan program güncellemeleri haftada bir yapılabilir.

Not: Güncelleme türleri ve seviyeleri hakkında ayrıntılı bilgi edinmek için lütfen [AVG Güncellemeleri](#) bölümünü inceleyin.

8.9.2. Güncelleme Yöneticisi Arayüzü



Güncelleme Yöneticisi'nin arayüzünde bileşenin fonksiyonları ve mevcut durumu hakkında bilginin yanı sıra (*Güncelleme Yöneticisi etkindir.*) ilgili istatistik bilgileri bulunmaktadır:

- **En son güncelleme** - veritabanının en son güncellendiği tarih ve saati gösterir.
- **Veritabanı sürümü**- en son virüs veritabanı sürümünün numarasını tanımlar ve bu numara virüs veritabanı her güncellendiğinde artar
- **Sonraki programlanan güncelleme** - Veritabanının yeniden güncellenmek için hangi tarih ve saatte programlandığını belirtir

Temel bileşen yapılandırma

İletişim kutusunun alt kısmında güncelleme işlemi kurallarında bazı değişiklikler yapabileceğiniz **Güncelleme Yöneticisi ayarları** bölümünü görebilirsiniz. Güncelleme dosyalarını otomatik olarak (**Güncellemeyi otomatik başlat**) ya da istek üzerine indirmeyi seçebilirsiniz. Varsayılan olarak **Güncellemeyi otomatik başlat** seçeneği

etkindir ve bu ayari degistirmeden muhafaza etmeniz önerilir! Güvenlik yazilimlarinin dogru sekilde çalismasi için en güncel güncelleme dosyalarinin düzenli araliklarla indirilmesi hayati önem tasir!

Bunun yani sira güncellemenin ne zaman baslatilacagini da belirleyebilirsiniz:

- o **Periyodik olarak** - zaman araligini belirleyin
- o **Belirli bir saatte** - kesin gün ve saati belirleyin

Varsayilan olarak her 4 saatte bir güncelleme islemi yapilir. Degistirmek için geçerli bir nedeniniz yoksa bu ayari oldugu sekilde muhafaza etmeniz önerilir!

Lütfen dikkat: Yazilim saticisi, en iyi performansin sunulabilmesi için tüm AVG bilesenlerini kurmustur. Bunun için iyi bir nedeniniz olmadikça AVG yapilandirmasini degistirmeyin. Ayarlarda yapılacak her tür degisiklik sadece deneyimli bir kullanıcı tarafından gerçekleştirilmelidir. AVG yapilandirmasini degistirmeniz gerekiyorsa sistem menüsünden ilgili ögeyi seçin **Araçlar/Gelismis ayarlar** ve yeni açilan [AVG Gelismis Ayarlar](#) iletisim kutusunda AVG yapilandirmasini düzenleyin.

Kontrol düğmeleri

Güncelleme Yöneticisi arayüzünde bulunan kontrol düğmeleri sunlardir:

- **Simdi güncelle** - istek üzerine [güncelleme islemini hemen](#) baslatir
- **Degisiklikleri kaydet** bu iletisim kutusunda yapılan her tür degisikligi kaydetmek ve uygulamak için bu düğmeye basin
- **İptal** - Varsayilan [AVG kullanıcı arayüzüne](#) dönmek için bu düğmeye basin (bilesenlere genel bakis)

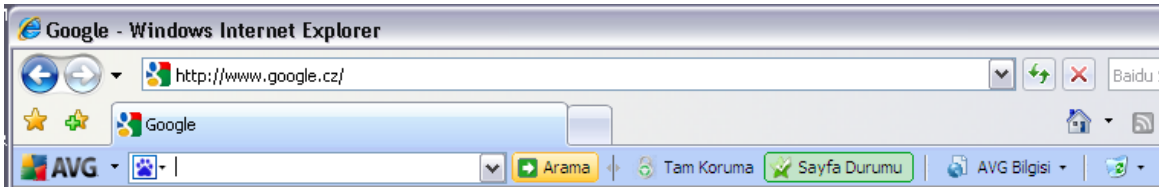
9. AVG Security Toolbar

AVG Security Toolbar **AVG Link Scanner** bileşeni ile çalışan yeni bir araçtır ve desteklenen Internet arama motorlarının (*Yahoo!*, *Google*, *Bing*, *Altavista*, *Baidu*) arama sonuçlarını kontrol eder. **AVG Security Toolbar** **AVG Link Scanner** işlevlerini kontrol etmek ve davranışını ayarlamak için kullanılabilir.

AVG 9 Anti-Virus yüklemesi sırasında araç çubuğunu yüklemeyi seçerseniz, web tarayicinize otomatik olarak eklenecektir. Baska bir Internet tarayicisi (örn. *Avant Browser*) kullanmanız durumunda beklenmeyen bir davranışla karşılaşabilirsiniz.

9.1. AVG Security Toolbar Arayüz

AVG Security Toolbar MS Internet Explorer (versiyon 6.0 ya da daha üstü) ve **Mozilla Firefox** (versiyon 2.0 ya da daha üstü) ile birlikte çalışacak şekilde tasarlanmıştır. **AVG Security Toolbar**'i yüklemeye karar verdiğinizde (**AVG yükleme işlemi** sırasında bileşeni yüklemek isteyip istemediğiniz sorulur), bileşen web tarayicinizde adres çubuğunun hemen altında bulunur:



Not: AVG Security Toolbar'in sunucu platformlarında kullanılması hedeflenmemiştir!

AVG Security Toolbar aşağıdakilerden oluşur:

- **AVG logo** - genel araç çubuğu öğelerine erişim sağlar. AVG web sitesine (<http://www.avg.com/>) yönlendirilmek için logo düğmesini tıklatın. AVG simgesinin yanındaki işaretçi tıklatıldığında aşağıdakiler açılır:
 - o **Araç Çubuğu Bilgisi** - araç çubuğunun koruyucu özelliklerinin yanı sıra **AVG Security Toolbar'in ana sayfasına giden bir bağlantı bulunur**
 - o **AVG 9 Anti-Virus** Ögesini Çalıştır - **AVG 9 Anti-Virus** kullanıcı arayüzünü açar
 - o **Seçenekler** - **AVG Security Toolbar** ayarlarınızı ihtiyaçlarınıza göre düzenleyebileceğiniz bir yapılandırma iletişim kutusu açar - bir sonraki konuya bakın: **AVG Security Toolbar Seçenekleri**
 - o **Geçmiş Sil** - AVG Security Toolbar'in *Tüm geçmişini sil* işlemini veya

Arama geçmişini sil, Tarayıcı geçmişini sil, İndirilen geçmişi sil ve Tanımlama bilgilerini sil işlemlerini uygulamanızı sağlar.

- o **Güncelleştir** - **AVG Security Toolbar için yeni güncelleştirmeleri kontrol eder**
- o **Yardım** - yardım dosyasını açmak, ürün geri bildirimini göndermek veya araç çubuğunun geçerli sürümünün ayrıntılarını görüntülemek için seçenekler sunar
- **Arama kutusu** - Arama kutusuna bir sözcük veya tümcecik girin. O anda hangi sayfa görüntüleniyorsa görüntülensin belirtilen arama motorunu kullanarak aramaya başlamak için ([AVG Security Toolbar Gelismis Seçenekler](#)'de hangi arama motorunu kullanmak istediğinizi belirtebilirsiniz ve Yahoo!, Wikipedia, Baidu, WebHledani veya Yandex'i seçebilirsiniz) **Ara**'ya basın. Ayrıca, arama kutusunda arama geçmişiniz de listelenir. Arama kutusundan yapılan aramalar {AVG Arama Kalkanı [korumasiyla analiz edilir](#).
- **Tam Koruma** - bu düğme yapılandırmaya bağlı olarak **Tam Koruma / Sinirli Koruma / Koruma Yok** şeklinde isteğe bağlı olarak görüntülenir **AVG 9 Anti-Virus**
- **Sayfa Durumu** - doğrudan araç çubuğunda olan bu düğme geçerli olarak karsıya yüklenen web sayfasının [AVG Search-Shield](#) bileşeni kriterine göre (sayfa güvenli / şüpheli / tehlikeli olabilir / tehlikeler içeriyor / taranamadı) değerlendirmesini görüntüler. Belirli web sitesi hakkında ayrıntılı veri içeren bir bilgi panelini açmak için düğmeyi tıklayın.
- **AVG Bilgileri** - AVG web sitesinde (<http://www.avg.com/>) bulunan önemli güvenlik bilgilerine bağlantılar sağlar.
 - o **Araç Çubuğu Bilgisi** - araç çubuğunun koruyucu özelliklerinin yanı sıra **AVG Security Toolbar'in ana sayfasına giden bir bağlantı bulunur**
 - o **Tehlikeler hakkında** - İnternet'teki geçerli virüsler ve tehlikeler hakkında bilgi sağlayarak AVG web sayfasını açar
 - o **AVG Haberler** - AVG ile ilgili en güncel basın açıklamalarını sağlayan web sayfasını açar
 - o **Geçerli Tehlike Düzeyi** - web'de geçerli tehlike seviyesinin grafik görünümünü içeren virüs laboratuvarı web sayfasını açar
 - o **Virüs Ansiklopedisi** - Belirli virüsleri ada göre arayabileceğiniz ve her biri

hakkında ayrıntılı bilgiler alabileceğiniz Virüs Ansiklopedisi sayfasını açar

9.2. AVG Security Toolbar Seçenekleri

Tüm **AVG Security Toolbar** parametrelerinin yapılandırmasına **AVG Security Toolbar** paneli içinden doğrudan erişilebilir. Düzenleme arayüzü, *Araç Çubuğu Seçenekleri* adlı yeni iletişim kutusunda dört bölüme ayrılarak **AVG / Seçenekler** araç çubuğu menü ögesinden açılır:

9.2.1. Genel Sekmesi



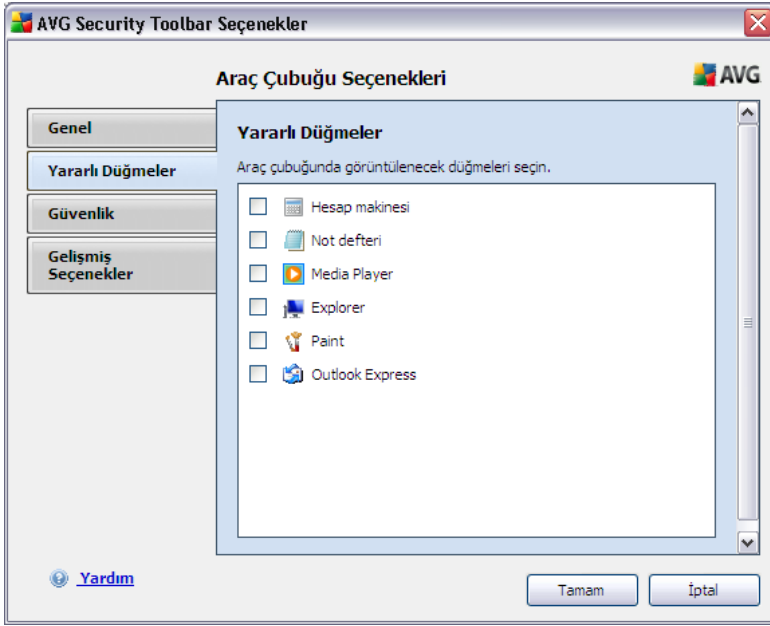
Bu sekmede, **AVG Security Toolbar** panelinden görüntülenmesi veya gizlenmesi gereken araç çubuğu kontrol düğmelerini belirtebilirsiniz. İlgili düğmeyi görüntülemek istediğiniz durumlarda seçeneğini işaretleyin. Her araç çubuğu düğmesinin işlevinin ayrıntılarını da bulabilirsiniz:

- **AVG Haberler Düğmesi** - düğme, AVG ile ilgili en son basın açıklamalarını içeren bir web sayfası açar
- **Haberler Düğmesi** - düğme, günlük basın haberlerine yapılandırılmış bir genel bakış sağlar
- **AVG Bilgi Düğmesi** - düğme, AVG araç çubuğu hakkında geçerli tehlikeler ve Internet tehlike düzeyi gibi bilgiler sağlar, virüs ansiklopedisini açar ve AVG

ürünleriyle ilgili daha fazla haber saglar

- **Geçmisi Sil Düğmesi** - Bu düğme Tüm geçmisi sil veya Arama geçmişini sil, Tarayici geçmişini sil, Indirme geçmişini sil veya Tanımlama bilgilerini sil işlemlerini dogrudan AVG Security Toolbar panelinden yapmanizi saglar.

9.2.2. Yararlı Düğmeler Sekmesi



Yararlı Düğmeler sekmesi, bir listeden uygulamalar seçmenizi ve simgelerinin araç çubuğu arayüzünde görüntülenmesini saglar. Simge, ilgili uygulamayı hemen baslatmak için hızlı bir bağlantı görevi görür.

9.2.3. Güvenlik Sekmesi



Güvenlik sekmesi iki bölüme ayrılmıştır, **AVG Tarayıcı Güvenliği** ve **Derecelendirmeler**, burada belirli onay kutularını kullanmak istediğiniz **AVG Security Toolbar** işlevselliğini ayarlamak için işaretleyebilirsiniz:

- **AVG Tarayıcı Güvenliği** - Bu öğeyi [AVG Arama Kalkanı](#) ve/veya [AVG Aktif Gezinme Kalkanı](#) hizmetini etkinleştirmek veya kapatmak için işaretleyin
- **Derecelendirmeler** - kullanmak istediğiniz [AVG Search-Shield](#) bileşeni yoluyla arama sonuçları derecelendirmeleri için kullanılan grafik sembolleri seçin:
 - o  sayfa güvenli
 - o  sayfa şüpheli gibi
 - o  sayfa tehlikeli olabilecek sayfalara bağlantılar içeriyor
 - o  sayfa etkin tehlikeler içeriyor
 - o  sayfaya erişilemedi ve bu yüzden taranamadı

Bu belirli tehlike seviyesi hakkında uyarılmak istendiginizi onaylamak için ilgili seçeneği işaretleyin. Ancak, etkin ve zararlı tehlikeleri içeren sayfalara atanan kırmızı isaretin görüntüsü kapatılamaz. **Tekrar, degistirmeniz için geçerli bir nedeniniz yoksa program satıcısı tarafından ayarlanan varsayılan yapılandırmayı korumanız önerilir.**

9.2.4. Gelişmiş Seçenekler Sekmesi



Gelişmiş Seçenekler sekmesinde ilk olarak varsayılan olarak hangi arama motorunu kullanmak istediğinizi seçin. *Yahoo!*, *Baidu*, *WebHledani* ve *Yandex* seçenekleriniz vardır. Varsayılan arama motorunu değiştirildiğinde değişikliğin etkili olabilmesi için lütfen Internet tarayicinizi yeniden başlatın.

Ayrıca, başka belirli **AVG Security Toolbar** ayarlarını da etkinleştirebilir veya kapatabilirsiniz:

- **Yahoo'yu Adres çubuğu için arama sağlayıcısı olarak ayarla ve sakla** - (varsayılan olarak açıktır) - İşaretliyse, bu seçenek bir arama anahtar kelimesini doğrudan Internet tarayicinizin adres çubuğuna ve Yahoo!'ya yazmanızı sağlar Hizmet ilgili web sitelerini otomatik olarak aramak için kullanılacaktır.
- **AVG'nin tarayıcı navigasyon hataları (404/DNS) hakkında öneride bulunmasına izin ver** - (varsayılan olarak açıktır) - web'de arama yaparken var olmayan veya görüntülenemeyen (404 hatası) bir sayfaya gelirsiniz,



otomatik olarak konuyla ilgili alternatif sayfaların bulunduğu bir web sayfasına yönlendirilirsiniz.

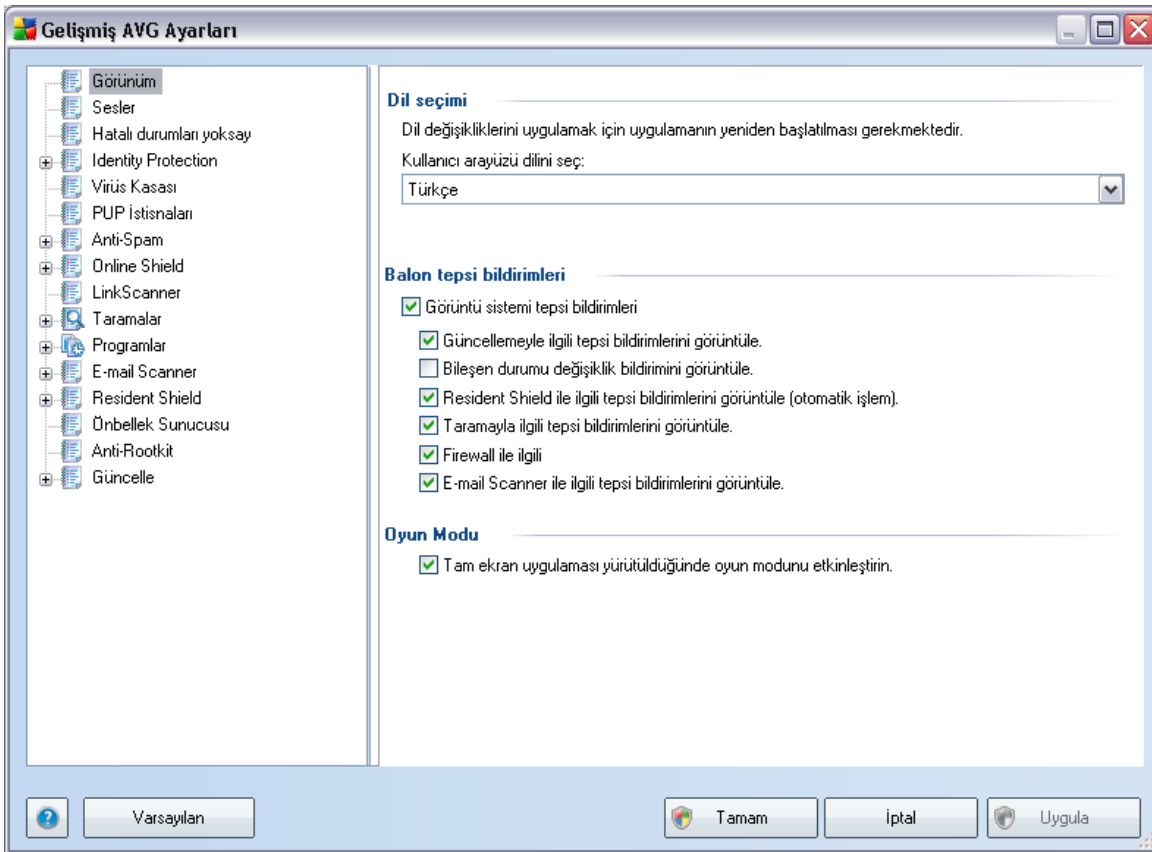
- **Yahoo'yu tarayıcım için arama sağlayıcısı olarak ayarla ve sakla** - (varsayılan olarak kapalıdır) - Yahoo! web arama için AVG Security Toolbar içinde varsayılan arama motorudur ve bu seçeneği etkinleştirdiğinizde web tarayıcısının varsayılan arama motoru da olabilir.
- **Gizliyen AVG Security Toolbar'i yeniden görüntüle (haftalık)** - (varsayılan olarak açıktır) - Bu seçenek varsayılan olarak etkindir ve **AVG Security Toolbar** 'iniz yanlışlıkla gizlendiğinde bir hafta içinde yeniden görüntülenecektir.

10. AVG Gelişmiş Ayarlar

AVG 9 Anti-Virus Gelişmiş yapılandırma iletişim kutusu **Gelişmiş AVG Ayarları** adlı yeni bir pencerede açılır. Pencere iki bölüme ayrılır: sol tarafta program yapılandırma seçeneklerini gösteren ağaç tipli menü bulunmaktadır. İletişim penceresini pencerenin sağ kısmında görüntülemek için *'nin ya da belirli bir bileşenin ()* yapılandırmasını değiştirmek istediğiniz bileşeni seçin.

10.1. Görünüm

Dolasım ağacının ilk ögesi olan **Görünüm**, [AVG kullanıcı arayüzünün](#) genel ayarlarına ve uygulamanın bazı temel seçeneklerine iliskindir:

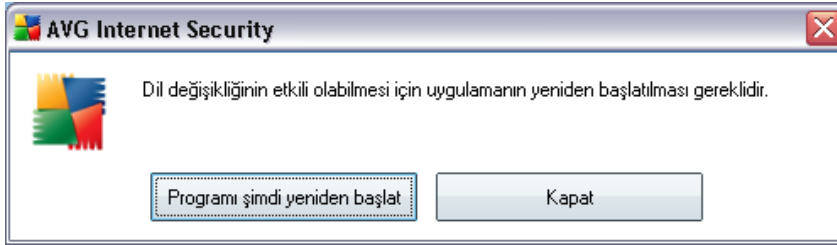


Dil seçimi

Dil seçimi bölümünde açılır menüden istediğiniz dili seçebilirsiniz; bunun ardından

seçtiğiniz dil tüm [AVG Kullanıcı Arayüzünde](#) kullanılacaktır. Açılır menü, sadece [Yükleme işlemi](#) sırasında yüklenmesini onayladığınız dilleri gösterir ([Özel Yükleme - Bileşen Seçimi](#) bölümünü inceleyiniz). Diğer bir yandan uygulamayı başka bir dile çevirme işlemini bitirmek için kullanıcı arayüzünü yeniden başlatmanız gerekir; aşağıdaki işlemleri takip edin:

- Uygulamada kullanılmasını istediğiniz dili seçin ve **Uygula** düğmesine (sağ alt köşede) basarak seçiminizi onaylayın.
- **Tamam** onay düğmesine basın
- AVG kullanıcı arayüzündeki dil değişiminin uygulamayı yeniden başlatmayı gerektirdiğini bildiren yeni iletişim kutusu penceresi açılır:



Balon tepsi bildirimleri

Bu bölümde uygulama durumu hakkında sistem tepsi üzerinde beliren balon bildirimlerini kaldırabilirsiniz. Balon bildirimlerinin varsayılan olarak görüntülenmesine izin verilir ve söz konusu yapılandırmanın değiştirilmemesi önerilir! Balon bildirimleri, genellikle AVG bileşenlerinin durum değişiklikleri hakkında bilgi verir ve bunlara dikkat etmeniz gerekir.

Diğer bir yandan, belirli bir neden dolayısıyla söz konusu bildirimlerin görüntülenmesini istemiyorsanız ya da sadece belirli bildirimlerin görüntülenmesini istiyorsanız (belirli AVG bileşenlerine ilişkin) tercihlerinizi aşağıdaki seçenekleri işaretleyerek ya da işaretlemeyerek tanımlayabilir ya da belirleyebilirsiniz:

- **Sistem tepsi bildirimlerini görüntüle** - Bu öğe varsayılan olarak işaretlidir (açıktır), ve bildirimler görüntülenir. Tüm balon bildirimleri kapatmak için bu öğenin işaretini kaldırın. Açıldığı zaman hangi bildirimlerin görüntüleneceğini seçebilirsiniz:
 - o [Güncelleme](#) hakkında bildirimleri görüntüle- AVG güncellemesi işleminin başlaması, ilerleyişi ve bitisi hakkında bilgilerin görüntülenmesini isteyip istemediğinize karar verin;

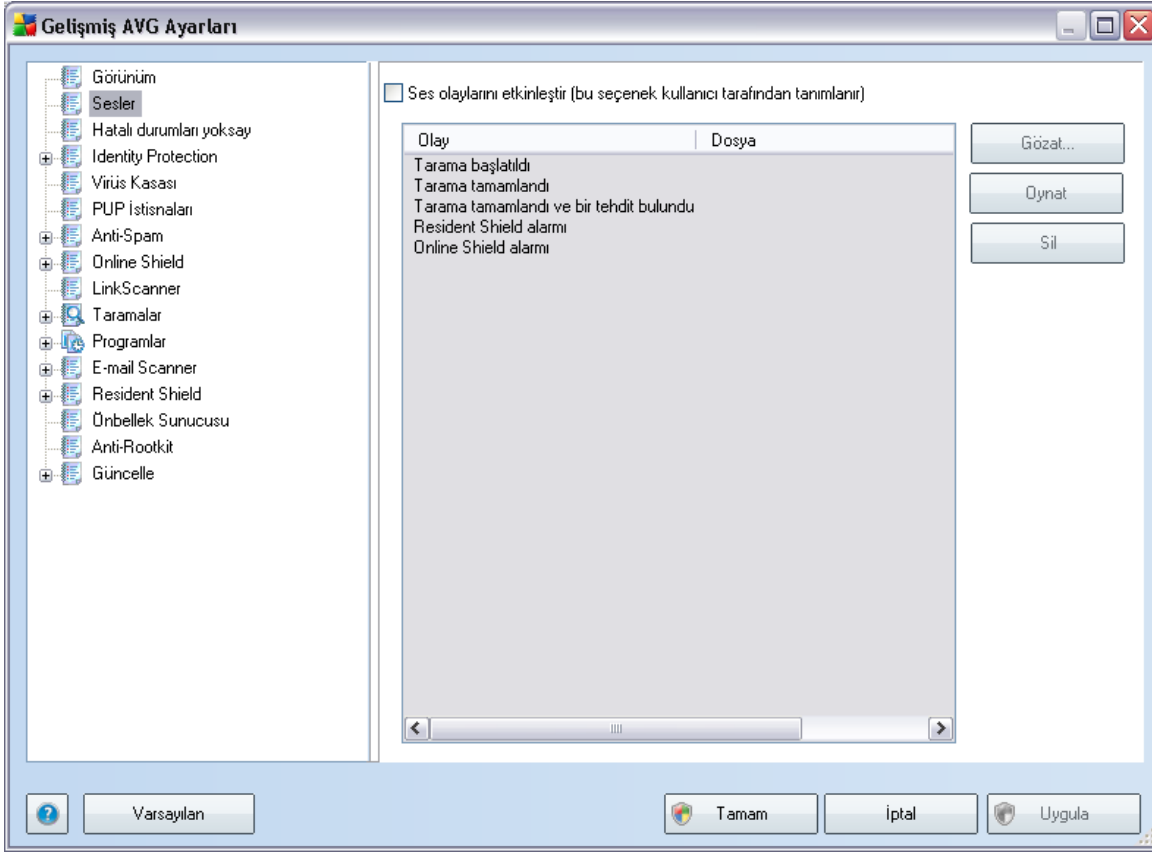
- o **Bilesen durum degisimi hakkında bildirimleri görüntüle** - Bilesenlerin aktif ya da pasif durumlarına ilişkin ya da muhtemel sorunları ile ilgili bildirimlerin görüntülenmesini isteyip istemediğinize karar verin. Bir bilesenin hata durumu rapor edilirken bu fonksiyon, [sistem tepsisi simgesinin](#) herhangi bir AVG bileseninde meydana gelen sorunu rapor ederken kullandığı bilgilendirici fonksiyonuna esdeğerdir (renk değişimi);
- o **Yerlesik Kalkanla ilgili tepsii bildirimlerini görüntüle** - kayıt, kopyalama ve açma işlemleriyle ilgili bilgilerin görüntülenmesi veya gizlenmesine (bu yapılandırma yalnızca Yerlesik Kalkan [Otomatik temizle seçeneği](#) açıksa gösterilir) karar verin;
- o **Tarama** hakkında bildirimleri görüntüle- Planlanan taramaların otomatik olarak başlaması, ilerleyişi ve sonuçları hakkında bilgilerin görüntülenmesini isteyip istemediğinize karar verin;
- o **E-posta Tarayıcısı ile ilgili tepsii bildirimlerini görüntüle** - gelen ve giden e-posta mesajlarının taranmasına ilişkin bildirimleri görüntülemek isteyip istemediğinize karar verin.

Oyun Modu

Bu AVG işlevi, olası AVG bilgi balonlarının (örn. zamanlanmış bir tarama başlatıldığında gösterilir) rahatsız edici olabileceği yerlerde (uygulamayı küçültebilir veya grafiklerini bozabilir) tam ekran uygulamalar için tasarlanmıştır. Bu durumdan kaçınmak için, **Tam ekran uygulama çalıştırılırken oyun modunu etkinleştir** seçeneği işaretli bırakın (varsayılan ayar).

10.2. Sesler

Sesler iletişim kutusu içinde, belirli AVG eylemleri hakkında bir ses bildirimiyle bilgilendirilmek isteyip istemediğinizi belirtebilirsiniz. İstiyorsanız, AVG eylemleri listesini etkinleştirmek için **Ses olaylarını etkinleştir** seçeneğini (varsayılan olarak kapalıdır) işaretleyin:

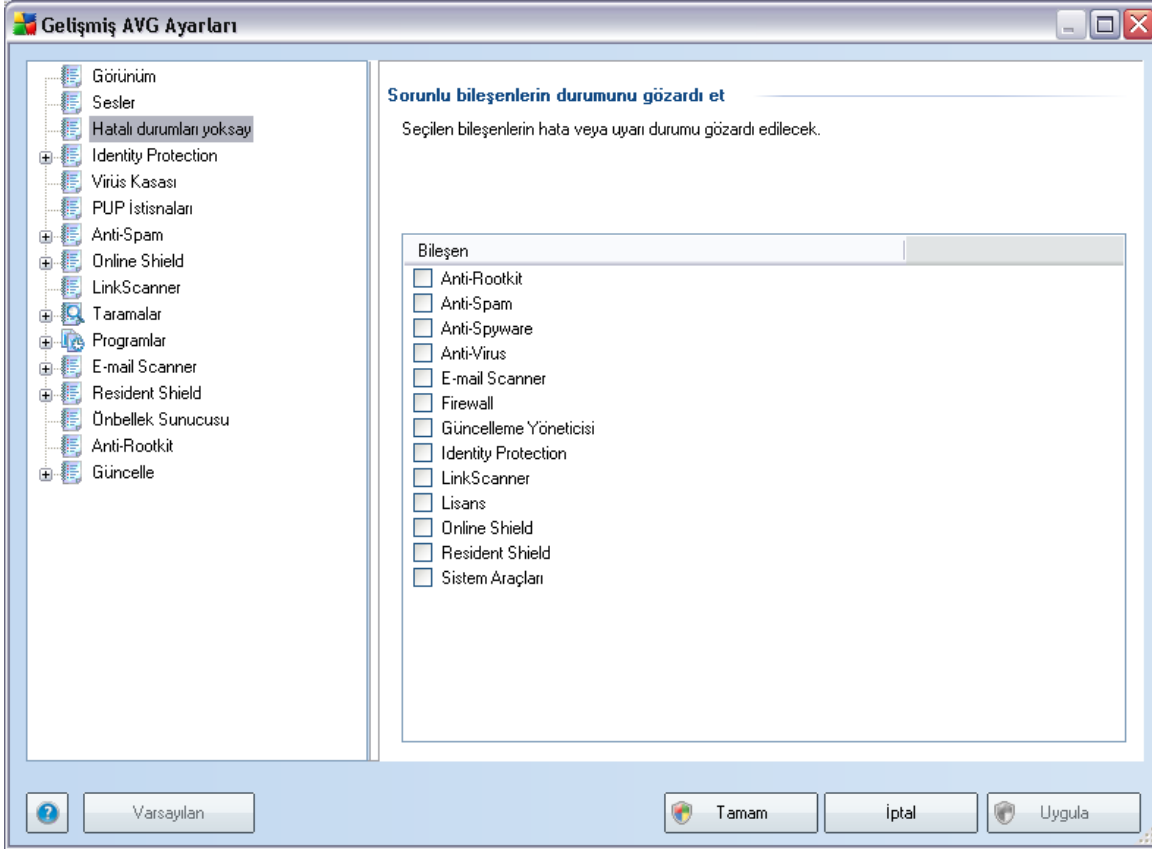


Sonra, ilgili olayı listeden seçin ve bu olaya atamak istediğiniz uygun ses için diskinize gözetin (**Gözet**). Seçili sesi dinlemek için, listede olayı vurgulayın ve **Çal** düğmesine basın. Belirli olaya atanan sesi kaldırmak için **Sil** düğmesini kullanın.

Not: Yalnızca *.wav sesleri desteklenir!

10.3. Hatalı Durumları Yoksay

Hatali bileşenleri göz ardı etme kosullari penceresinde, bilgilendirilmek istemediginiz bileşenleri seçebilirsiniz:



Öntanımlı olarak listede herhangi bir bileşen seçilmemistir. Bileşenlerden herhangi biri hatalı duruma düşerse aşağıdaki yöntemlerden biri vasıtasıyla uyarılacaksınız demektir:

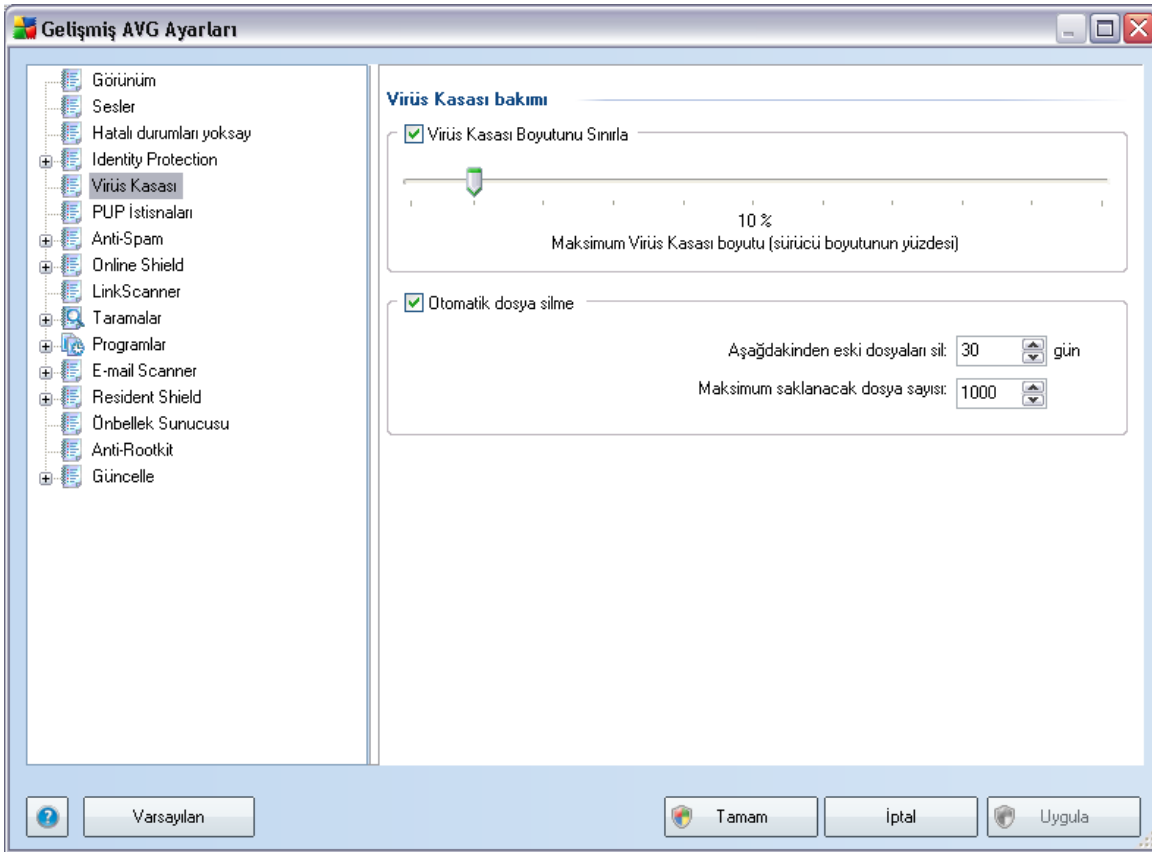
- **sistem tepsisi simgesi** - AVG'nin tüm bileşenleri doğru şekilde çalışırken simge, 4 renkli görünecektir ancak herhangi bir aksaklık olursa simgenin yanında sarı bir ünlem işareti görülür,
- AVG ana penceresinin **Güvenlik Durumu Hakkında Bilgi** bölümünde mevcut sorun açıklanır

Bileşenlerden birini geçici bir süre ile kapatmanız gereken bir durum ile karşılaşabilirsiniz(*bileşenlerin geçici süre ile kapatılması önerilmemektedir, tüm bileşenleri daima açık*)

durumda ve öntanımlı yapılandırmayı muhafaza etmeniz gerekir ancak aksi durumlarla karşılaşabilirsiniz). Bu durumda sistem tepsisi simgesi, otomatik olarak bileşenin hata durumunda olduğunu bildirir. Ancak bu durumda gerçek bir hatadan söz edemeyiz çünkü hatayı siz başlatmışsınızdır ve potansiyel riskin farkında olmalısınız. Aynı zamanda simge gri renkli görüntüledikten sonra daha sonra vuku bulacak hataları rapor etmeyecektir.

Bu durumda yukarıdaki pencerece hata durumunda olan (ya da kapatılmış) bileşenleri seçebilirsiniz ve söz konusu durum hakkında bilgilendirilmek istemeyebilirsiniz. **Bileşen durumunun gözardı edilmesi** işlemi doğrudan [AVG ana penceresinin bileşenlere genel bakış](#) penceresinden de gerçekleştirilebilir.

10.4. Virüs Kasası



Virüs Kasası bakımı iletişim kutusu, [Virüs Kasası](#)'nda depolanan nesnelerin yönetimi hususunda çeşitli parametreleri tanımlayabilmenizi sağlar:

- **Virüs Kasası boyutunu sınırla** - [Virüs Kasası](#)'nin maksimum boyutu için

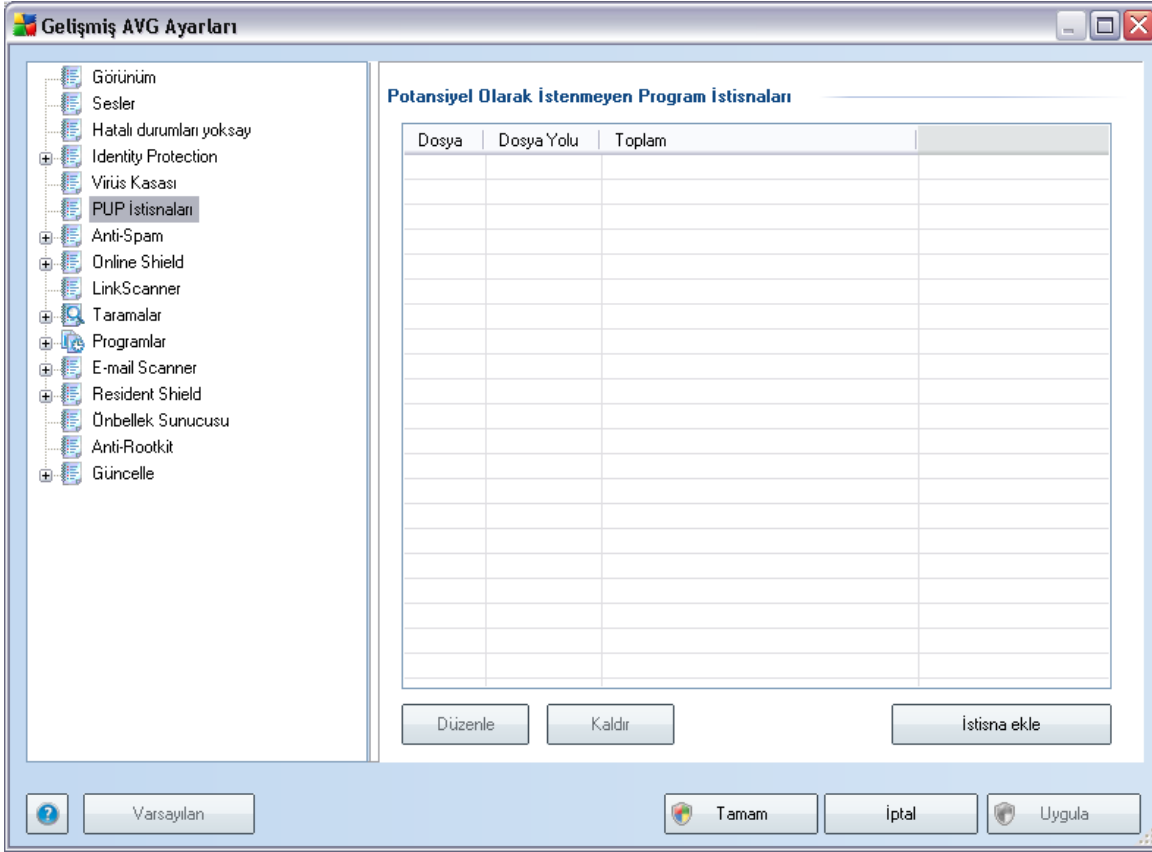


kaydırıcıyı kullanın. Söz konusu boyut, sabit diskinizin boyutu ile doğru orantili olacaktır.

- **Otomatik dosya silme** - bu bölümde nesnelerin [Virüs Kasasında](#) depolanacakları maksimum süreyi (... **Günden eski dosyaları sil**), [Virüs Kasasında](#) depolanacak maksimum dosya sayısını(**Depolanacak maksimum dosya sayısı**) belirleyebilirsiniz.

10.5. PUP İstisnaları

AVG 9 Anti-Virus, bunun yanı sıra sistemde potansiyel anlamda istenmeyen çalıştırılabilir uygulamaları ya da DLL kütüphanelerini de inceleyebilmekte ve tespit edebilmektedir. Bazı durumlarda kullanıcı belirli istenmeyen programların (*bilerek yüklenen programlar*) bilgisayarında bulunmasını tercih edebilir. Bunlardan bazıları reklam yazılımları ve özellikle ücretsiz yazılımlardır. Söz konusu reklam yazılımları AVG tarafından tespit edilip **potansiyel olarak istenmeyen program** statüsü ile rapor edilebilir. Söz konusu programın bilgisayarınızda bulunmasını istiyorsanız ilgili programı, potansiyel olarak istenmeyen program istisnası şeklinde atayabilirsiniz.

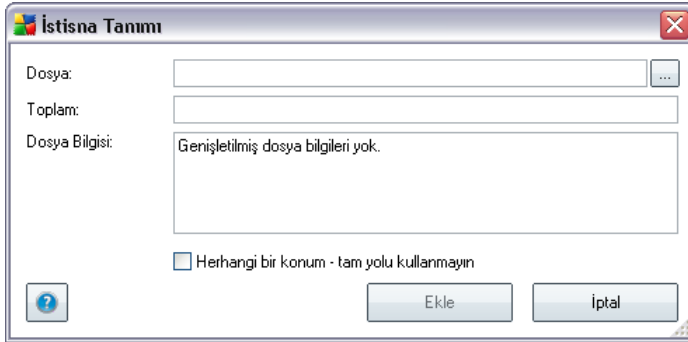


Potansiyel Olarak İstenmeyen Program İstisnaları iletişim kutusunda, potansiyel olarak istenmeyen programlardan tanımlanan ve mevcut durumda geçerli istisnalar bulunmaktadır. Listeyi düzenleyebilir, varolan öğeleri silebilir veya yeni istisnalar ekleyebilirsiniz. Aşağıdaki bilgiler her bir istisna için listede bulunabilir:

- **Dosya** - İlgili uygulamanın adını sağlar
- **Dosya Yolu** - Uygulamanın konumuna olan yolu gösterir
- **İmzayı Kontrol Et** - seçilen dosyanın 'imzasını' görüntüler. Bu sağlama, AVG'nin seçilen dosyayı diğer dosyalardan ayırmasını sağlamak üzere otomatik oluşturulan karakter satırlarından meydana gelmektedir. Sağlama, dosyanın başarıyla eklenmesinin ardından oluşturulur ve görüntülenir.

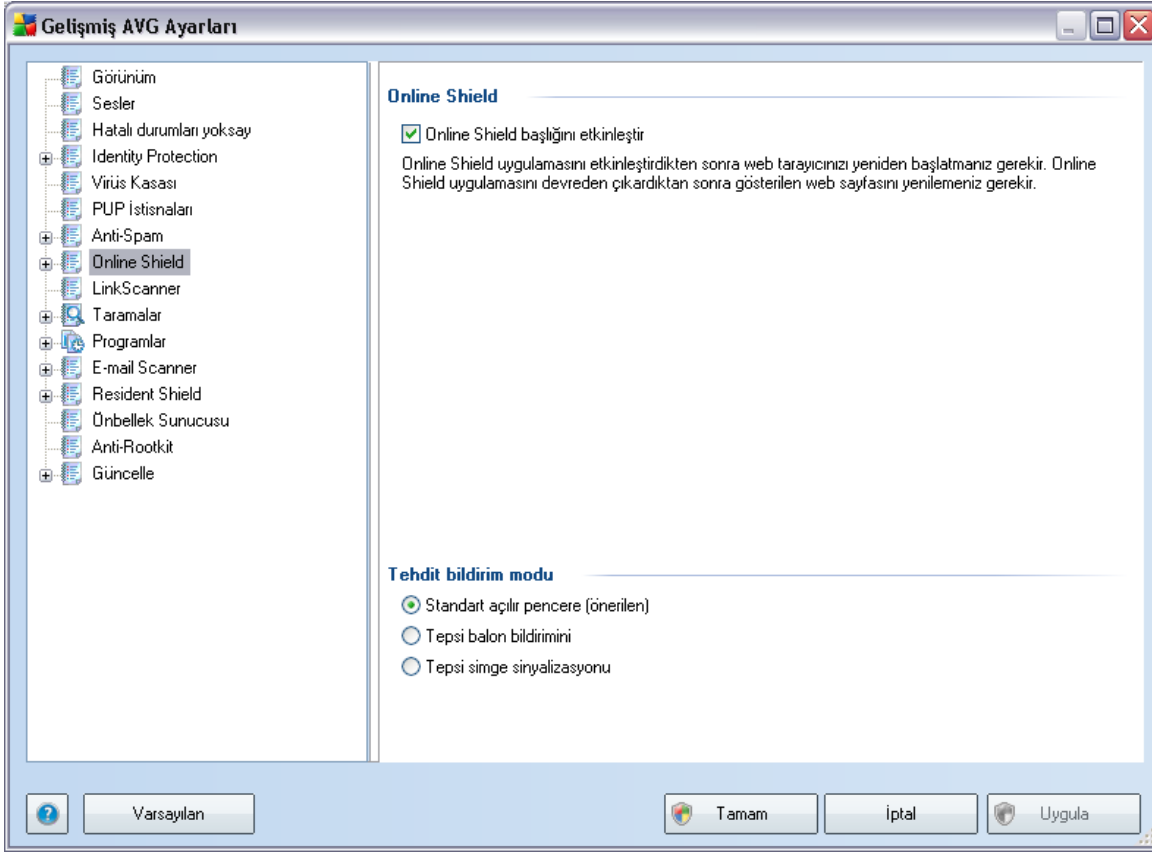
Kontrol düğmeleri

- **Düzenle** - önceden tanımlanmış olan bir istisnanın parametrelerini düzenleyebileceğiniz bir düzenleme iletişim kutusu açar (*yeni istisna tanımlama iletişim kutusuyla aynı, aşağıya bakın*)
- **Sil** - seçilen öğeyi istisnalar listesinden siler
- **İstisna ekle** - oluşturulacak yeni istisnanın parametrelerini tanımlayabileceğiniz yeni bir düzenleme iletişim kutusu açar:



- o **Dosya** - istisna olarak belirlemek istediğiniz dosyanın tam yolunu girin
- o **İmzayı Kontrol Et** - seçilen dosyanın "özel imzasını" görüntüler. Bu sağlama, AVG'nin seçilen dosyayı diğer dosyalardan ayırmasını sağlamak üzere otomatik oluşturulan karakter satırlarından meydana gelmektedir. Sağlama, dosyanın başarıyla eklenmesinin ardından oluşturulur ve görüntülenir.
- o **Dosya Bilgisi** - dosya hakkında (*lisans/sürüm bilgileri, vb*) mevcut tüm bilgileri görüntüler
- o **Herhangi bir yerde - tam yolu kullanma** - söz konusu dosyayı sadece belirli bir konumda istisna olarak atamak istiyorsanız bu kutucuğu işaretlemeyi bırakın

10.6. Çevrimiçi Kalkan



Web Korumasi iletişim kutusu **Online Shield'i etkinleştir** seçeneğiyle (*varsayılan olarak etkin*) tüm **Online Shield** bileşenini etkinleştirmenizi/devre dışı bırakmanızı sağlar. Bu bileşenin daha fazla gelişmiş ayarını görmek için lütfen gezinti ağacında listelenen ardışık iletişim kutularına bakın:

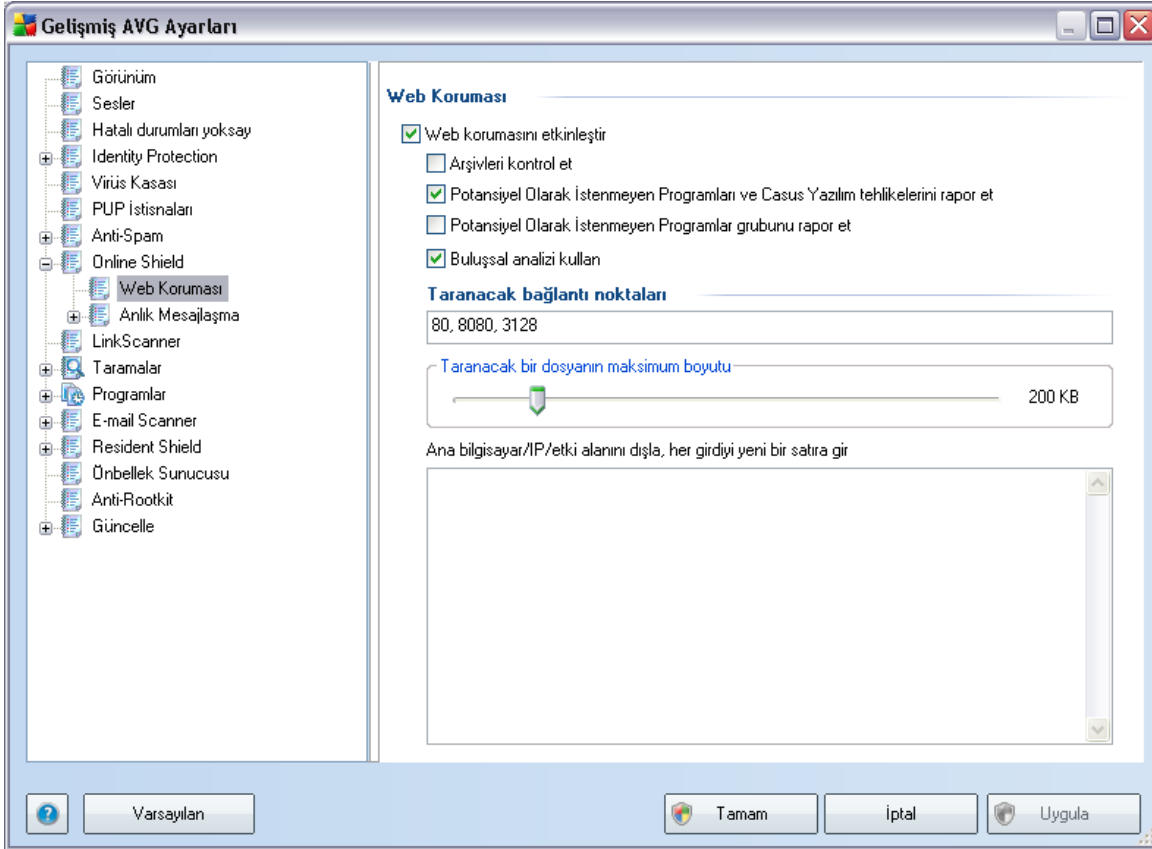
- [Web Korumasi](#)
- [Anlık Mesajlaşma](#)

Tehlike bildirme modu

İletişim kutusunun alt kısmında algılanması muhtemel tehdit hakkında ne şekilde bilgilendirilmek istediğinizi seçin: standart açılır iletişim kutusuyla, tepsi balon bildirimiyle

ya da tepsi simgesi bilgileriyle.

10.6.1. Web Koruması



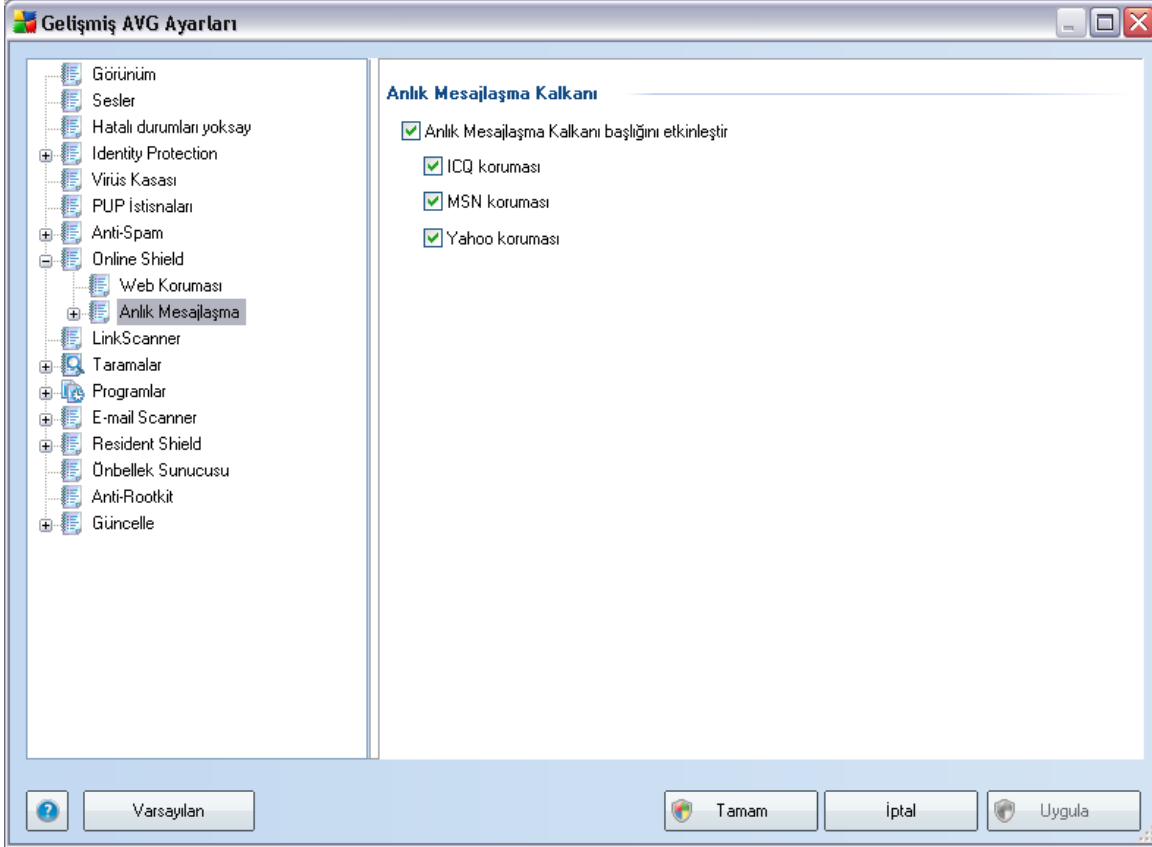
Web Koruması- web sitelerinin içeriğinin taranmasına ilişkin bileşen yapılandırmasını düzenleyebilirsiniz. Düzenleme arayüzü ile aşağıdaki temel seçenekleri yapılandırabilirsiniz:

- **Web korumasını etkinleştir** - bu seçenek [Online Shield](#)'in www sayfalarının içeriğinin taranmasını gerçekleşmek gerektiğini onaylar. Bu seçeneğin etkin konumda olmasına rağmen (*varsayılan olarak*) söz konusu öğeleri açık kapatabilirsiniz:
 - o **Arsivleri kontrol et** - görüntülenecek www sayfasında bulunan arşivlerin içeriğini tarar.
 - o **Potansiyel Olarak İstenmeyen Programları ve Casus Yazılım**

tehlikelerini rapor et - (varsayılan olarak açıktır): [Anti-Spyware](#) motorunu etkinleştirmek ve virüslerle birlikte casus yazılımları da kontrol etmek için isaretleyin. [Casus yazılım](#), kötü amaçlı yazılım olabilecek kategorisini temsil eder: bir güvenlik riski oluştursa da bu programlardan bazıları bilerek yüklenebilir. Bilgisayarınızın güvenliğini artırdığından, bu özelliği etkin durumda tutmanızı öneriyoruz.

- o **Gelişmiş Potansiyel Olarak İstenmeyen Programlar setini bildir** - önceki seçenek etkinleştirilirse, genişletilmiş [casus yazılım](#) paketini algılamak için bu kutuyu da isaretleyebilirsiniz: doğrudan üreticiden alınan tamamen zararsız olan, ancak daha sonra kötüye kullanılan programlar. Bu, bilgisayar güvenliğinizi daha da artıran ek bir önlemdir, ancak yasal programları da engelleyebilir ve bu yüzden varsayılan olarak kapalıdır.
- o **Bulgusal analizi kulan-** görüntülenecek web sitesinin içeriği [bulussal analiz](#) yöntemi kullanılarak taranır (*taranan nesnenin sanal bir bilgisayar ortamında dinamik olarak canlandırılmasına ilişkin talimatlar*).
- o **Taranacak bağlantı noktaları** - bu alanda standart http iletişimi için kullanılan bağlantı noktaları listelenir. Bilgisayar konfigürasyonunuz farklı ise bağlantı noktalarını istediğiniz şekilde değiştirebilirsiniz.
- o **Taranacak maksimum dosya bölümü büyüklüğü** - Dahil edilen dosyalar görüntülenen sayfada mevcutsa, bunları bilgisayarınıza indirmeden önce de içeriklerini tarayabilirsiniz. Ancak büyük dosyaların taranması zaman alabilir ve web sayfasının indirilmesi de önemli ölçüde yavaşlayabilir. [Online Shield](#) ile taranacak dosyanın maksimum boyutunu belirlemek için kaydırma çubuğunu kullanabilirsiniz. İndirilen dosya belirtilen dosya boyutundan daha büyük olsa ve buna bağlı olarak Online Shield ile taranmaya bile korunmaya devam edersiniz: dosya, bulasmis olması halinde [Yerlesik Kalkan](#) tarafından tespit edilecektir.
- o **Barındırma/IP/etki alanını dışla** - metin alanına Online Shield tarafından taranmasını istemediğiniz bir sunucunun tam adını ([barındırma, IP adresi, maskeli IP adresi ya da URL](#)) ya da etki alanı adını girin. Bu nedenle, bu işlemi yapmadan önce web sitesinin içeriğinin zararlı olmadığından emin olmanız gerekir.

10.6.2. Anlık Mesajlaşma

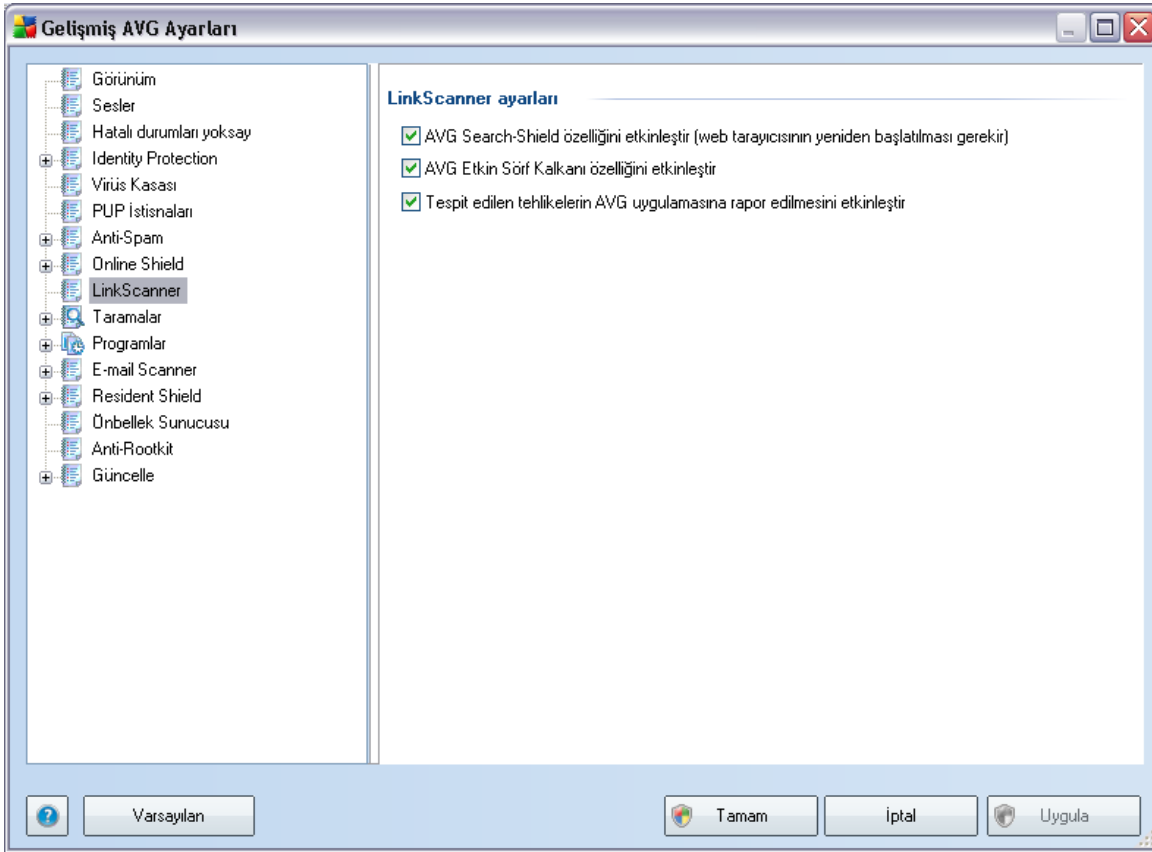


Anlık Mesajlaşma Kalkanı iletişim kutusunda anlık mesajlaşmaların taranmasına ilişkin **Online Shield** bileşeninin ayarlarını yapabilirsiniz. Geçerli olarak aşağıdaki üç anlık mesajlaşma programı desteklenmektedir: **ICQ**, **MSN** ve **Yahoo** - Online Shield'in çevrimiçi görüşmelerinizin virüssüz olmadığını doğrulamasını istiyorsanız ilgili öğeleri işaretleyin. ***

İzin verilen/engellenen kullanıcılara ilişkin ayarlar hususunda ilgili iletişim kutusunu görüntüleyebilir ya da düzenleyebilirsiniz (**Gelişmiş ICQ**, **Gelişmiş MSN**, **Gelişmiş Yahoo**) ve **Beyaz Listeyi** (sizinle iletişim kurmasına izin verilen kullanıcıların listesi) ve **Kara Listeyi** (engellenmesini istediğiniz kullanıcıların listesi) oluşturabilirsiniz.

10.7. Bağlantı Tarayıcı

LinkScanner ayarları iletişim kutusu, **LinkScanner**'in temel özelliklerini açıp kapatmanızı sağlar:



- **AVG Search-Shield'i Etkinleştir** - (varsayılan olarak açıktır): arama motorunca getirilen sitelerin içeriğinin önceden kontrol edildiğine dair Google, Yahoo, Bing, Yandex, Altavista veya Baidu'da gerçekleştirilen aramalara ilişkin bilgilendirici simgeler.
- **AVG Search-Shield'i etkinleştir** - (varsayılan olarak açıktır): erişim sağlandığı anda güvenlik açığı olan web sitelerine karşı koruma (gerçek zamanlı) sağlamak için etkinleştirin. Bilinen zararlı site bağlantıları ve zararlı içerikleri, kullanıcı tarafından bir web tarayıcısı(ya da HTTP kullanan diğer bir program) üzerinden erişim sağlandığı anda engellenir.
- **Algılanan tehlikelerin AVG'ye rapor edilmesini etkinleştir** - (varsayılan



olarak aıktır): **AVG Active Surf-Shield** veya **AVG Search-Shield** yoluyla kullanıcıların bulduğu güvenlik aıklarının ve kötü sitelerin rapor edilmesini sağlamak amacıyla web'deki zararlı etkinlikler hakkında veritabanına bilgi toplamak için bu ögeyi işaretleyin.

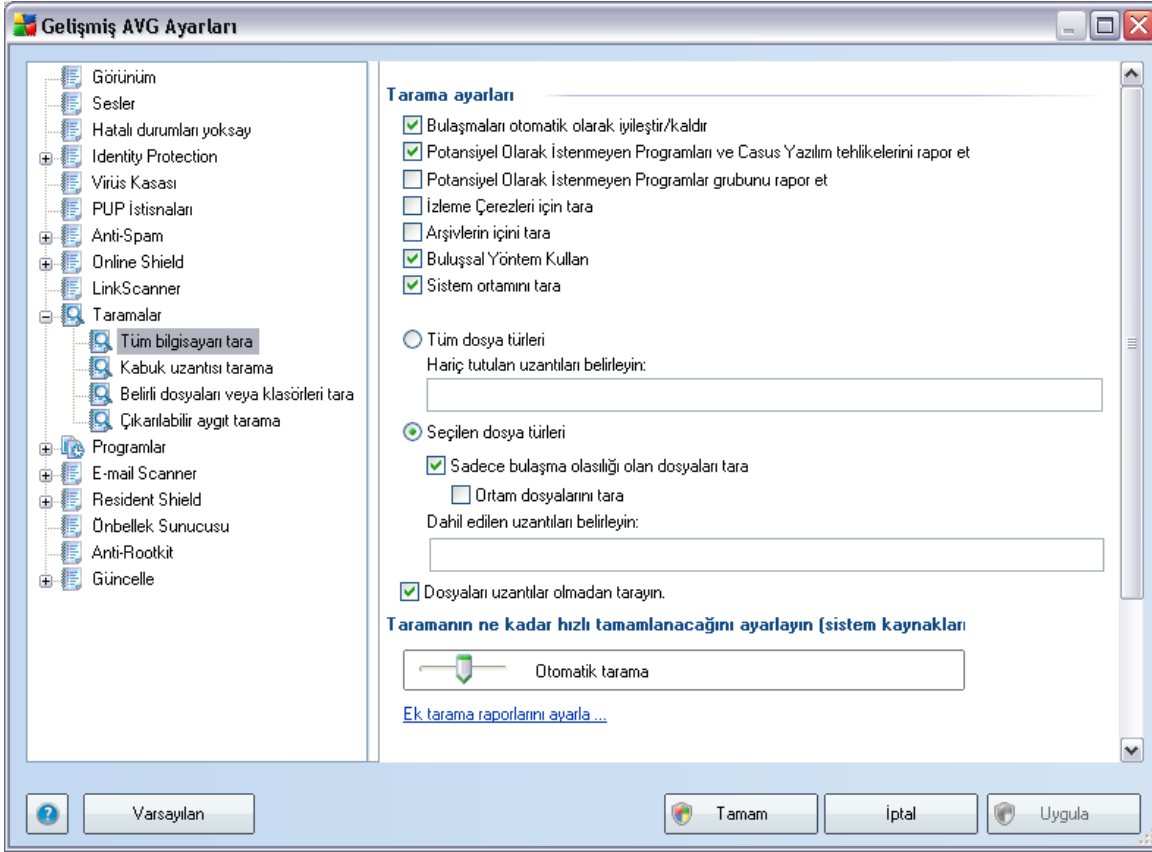
10.8. Taramalar

Gelişmiş tarama ayarları, yazılım geliştiricisi tarafından tanımlanan belirli tarama türlerine ilişkin üç kategoriye bölünmüştür:

- **Tam Bilgisayar Taraması** - bilgisayarın tamamen tarandığı standart öntanımlı taramadır
- **Kabuk Uzanti Taraması** - seçilen nesnenin doğrudan Windows Explorer ortamında taraması işlemidir
- **Belirli Dosya ya da Klasörlerin Taranması** - bilgisayarınızın seçilen alanlarının tarandığı standart öntanımlı taramadır
- **Çıkarılabilir Aygıt Taraması** - bilgisayarınıza bağlanan çıkarılabilir aygıtların taraması işlemidir

10.8.1. Tüm Bilgisayarı Tara

Bilgisayarın tümünü tara seçeneği, yazılım satıcısı tarafından belirlenmiş öntanımlı tarama yöntemlerinden birinin parametrelerini düzenleyebilmenize olanak tanır, **Bilgisayarın tümünün taranması**:



Tarama ayarları

Tarama ayarları bölümünde isteğe bağlı olarak açılıp kapatılabilecek tarama parametreleri listelenmiştir:

- **Bulaşmayı otomatik temizle/sil** : tarama işlemi sırasında bir virüs tanımlanırsa ve temizlenmesi mümkün ise otomatik olarak temizlenir. Bulaşmış dosya otomatik olarak temizlenemezse, bulaşmış nesne **Virüs Kasası**'na taşınır.
- **Potansiyel Olarak İstenmeyen Programları ve Casus Yazılım tehlikelerini rapor et** - (varsayılan olarak açıktır): **Anti-Spyware** motorunu etkinleştirmek ve virüslerle birlikte casus yazılımları da kontrol etmek için işaretleyin. **Casus yazılım**, kötü amaçlı yazılım olabilecek kategorisini temsil eder: bir güvenlik riski oluştursa da bu programlardan bazıları bilerek yüklenebilir. Bilgisayarınızın güvenliğini artırdığından, bu özelliği etkin durumda tutmanızı öneriyoruz.

- **Gelismis Potansiyel Olarak Istenmeyen Programlar setini bildir** - önceki seçenek etkinleştirilirse, genişletilmiş [casus yazılım](#) paketini algılamak için bu kutuyu da işaretleyebilirsiniz: doğrudan üreticiden alınan tamamen zararsız olan, ancak daha sonra kötüye kullanılan programlar. Bu, bilgisayar güvenliğinizi daha da artıran ek bir önlemdir, ancak yasal programları da engelleyebilir ve bu yüzden varsayılan olarak kapalıdır.
- **Tanımlama Bilgilerini Tara** - [Casus Yazılımdan Koruma](#) bileşeninin bu parametresi, tarama sırasında tespit edilmesi istenen tanımlama bilgilerini tanımlar (*HTTP tanımlama bilgileri site tercihleri ya da elektronik alışveriş sepeti içeriği gibi kullanıcı hakkında belirli bilgilerin toplanması, temin edilmesi ve izlenmesi için kullanılır*)
- **Arsivleri tara** - bu parametre, ZIP, RAR vb. arşiv dosyalarının içinde sıkıştırılmış dosyaların bile taranmasını sağlar.
- **Bulgusal Analiz Kullan** - bulgusal analiz (*taranan nesnenin sanal bir bilgisayar ortamında dinamik olarak canlandırılması'na ilişkin talimatlar*) tarama sırasında kullanılacak virüs tespiti yöntemlerinden birisidir;
- **Sistem ortamını tara** : tarama işlemi, bilgisayarınızın sistem alanlarını da kontrol edecektir.

Ayrıca, taramak isteyip istemediğinize karar vermelisiniz

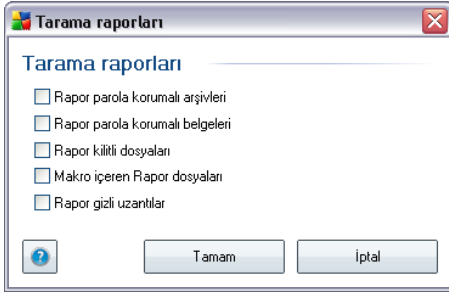
- **Tüm dosya türleri** , virgülle ayrılmış (*kaydedilirken virgüller noktalı virgüle dönüşür*) dosya uzantıları listesi sağlayarak taramadan hariç tutulacakların taranmaması için tanımlama olasılığı sağlar;
- **Seçili dosya türleri** - Yalnızca virüs bulaşabilme olasılığı olan dosyaları taramayı istediğinizi belirtebilirsiniz (*virüs bulaşmayan dosyalar taranmayacaktır, örneğin, bazı düz metin dosyaları veya bazı diğer çalıştırılmayan dosyalar*); ortam dosyaları (*video, ses dosyaları - bu onay kutusunun işaretini kaldırırsanız, bu dosyalar genellikle çok büyük olduğundan ve virüs bulaşma olasılıkları çok az olduğundan tarama süresini daha da azaltır*). Tekrar, her zaman taranması gereken dosyaları uzantılarına göre belirtebilirsiniz.
- İsteğe bağlı olarak, **Uzantıları olmayan dosyaları taramaya** da karar verebilirsiniz - bu seçenek varsayılan olarak açıktır ve gerçekten bir nedeniniz yoksa değiştirmemeniz önerilir. Uzantısı olmayan dosyalar süpheli olabilir ve her zaman taranmalıdır.

Tarama işlemi önceliği

Tarama işlemi önceliği bölümünde, sistem kaynakları kullanımına bağlı olarak istediğiniz tarama hızını seçebilirsiniz. Varsayılan olarak bu seçenek değeri, otomatik kaynak kullanımının ortalama düzeyine ayarlıdır. Tarama işleminin daha hızlı ilerlemesini istiyorsanız tarama işlemi daha kısa sürecektir fakat tarama işlemi sırasında sistem kaynakları oldukça yüklü bir şekilde kullanılacak ve bilgisayar üzerindeki diğer işlemleri yavaşlatacaktır (*bu seçenek bilgisayarınız açıkken kullanılmadığı sırada seçilebilir*). Öte yandan tarama süresini uzatarak da sistem kaynaklarının kullanımını azaltabilirsiniz.

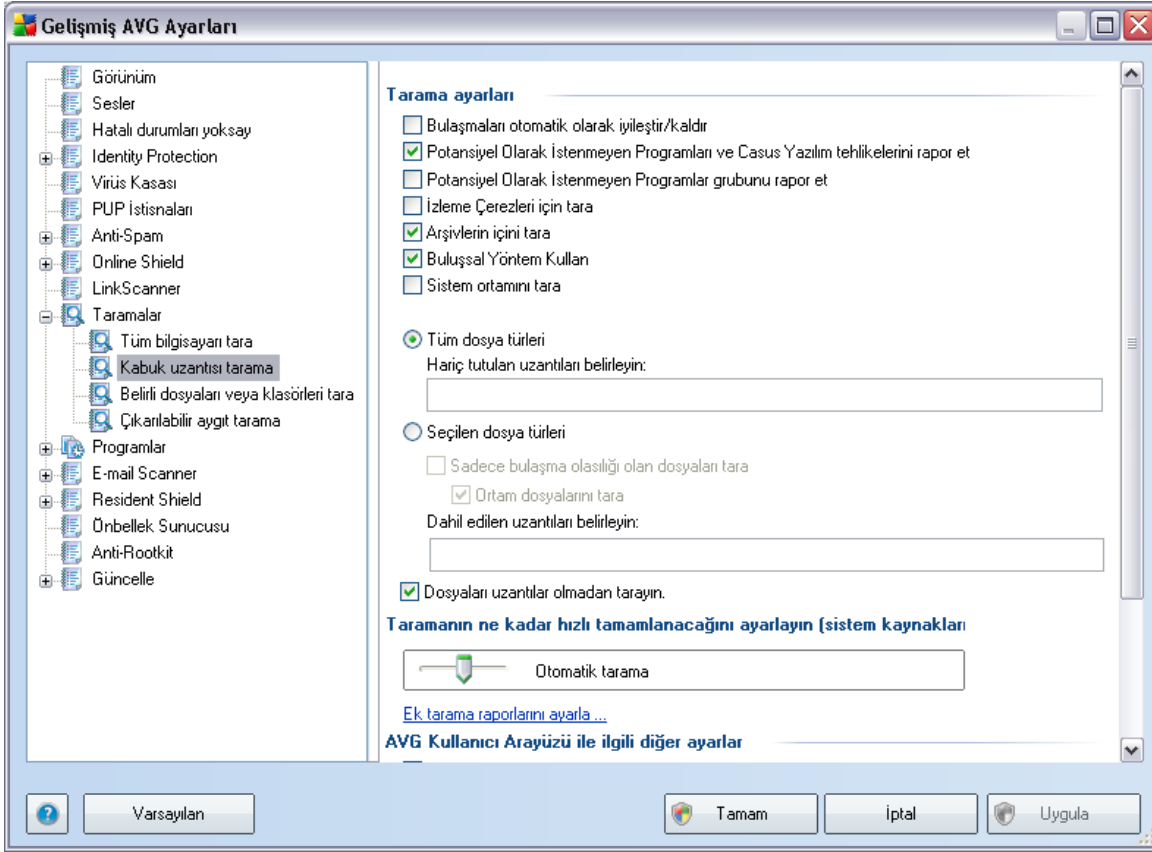
Ek tarama raporlarını ayarla ...

Diger tarama raporlarını belirle ... bağlantısına tıklayarak hangi tarama bulgularının rapor edileceğine ilişkin seçimleri yapabileceğiniz **Tarama raporları** iletişim kutusu penceresini açabilirsiniz:



10.8.2. Kabuk Uzantısı Tarama

Daha önce bahsettiğimiz [Tam bilgisayar taraması](#) ögesine benzer olan bu öge, **Kabuk uzantı taraması** olarak adlandırılır ve yazılım satıcısı tarafından öntanımlı olarak belirlenmiş tarama parametrelerine ek olarak çok daha fazla sayıda seçenek sunar. Bu sefer, yapılandırma [doğrudan Windows Gezgini üzerinden baslatılan belirli nesnelerin taraması](#) esasına dayanmaktadır (*kabuk uzantısı*), [Windows Gezgini'nde Tarama](#) bölümüne bakın:

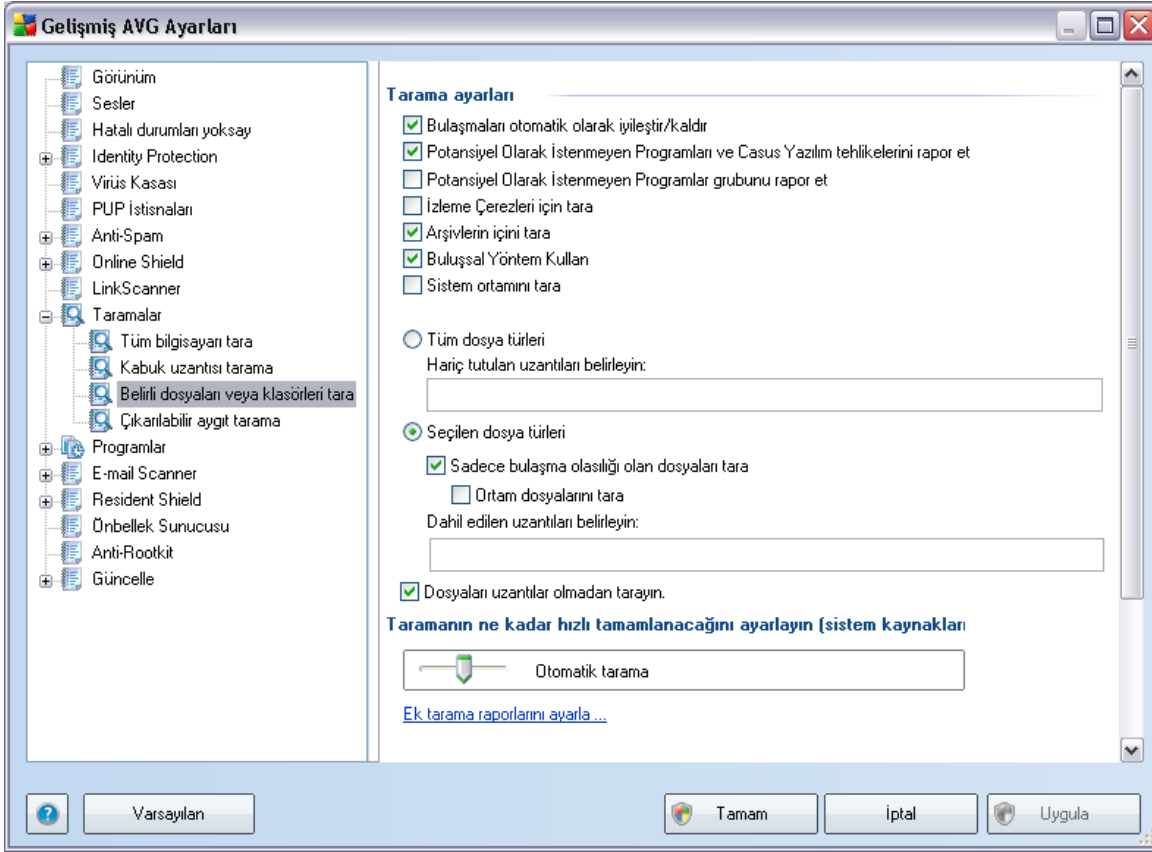


Parametre listesi, [Tüm bilgisayarı tarama](#) ögesinin parametre listesi ile aynıdır. Diğer bir yandan varsayılan ayarlar farklılık göstermektedir: **Tüm Bilgisayar taramasında** parametrelerin çoğu seçilmiştir ancak **Kabuk uzantısı taramasında** ([Windows Gezgini Taraması](#)) sadece ilgili parametreler etkinleştirilmiştir.

Not: Belirli parametrelerin tanımlar hususunda bilgi almak için [AVG Gelişmiş Ayarlar / Taramalar / Tüm Bilgisayar Taraması](#) bölümünü inceleyin.

10.8.3. Belirli Dosyaları veya Klasörleri Tara

Belirli dosya ya da klasörleri tara fonksiyonunun düzenleme arayüzü [Tüm Bilgisayar Taraması](#) fonksiyonunun düzenleme penceresi ile aynıdır. Tüm konfigürasyon seçenekleri aynıdır; diğer bir yandan [Tüm bilgisayar taraması](#) için varsayılan ayarlar daha keskindir:

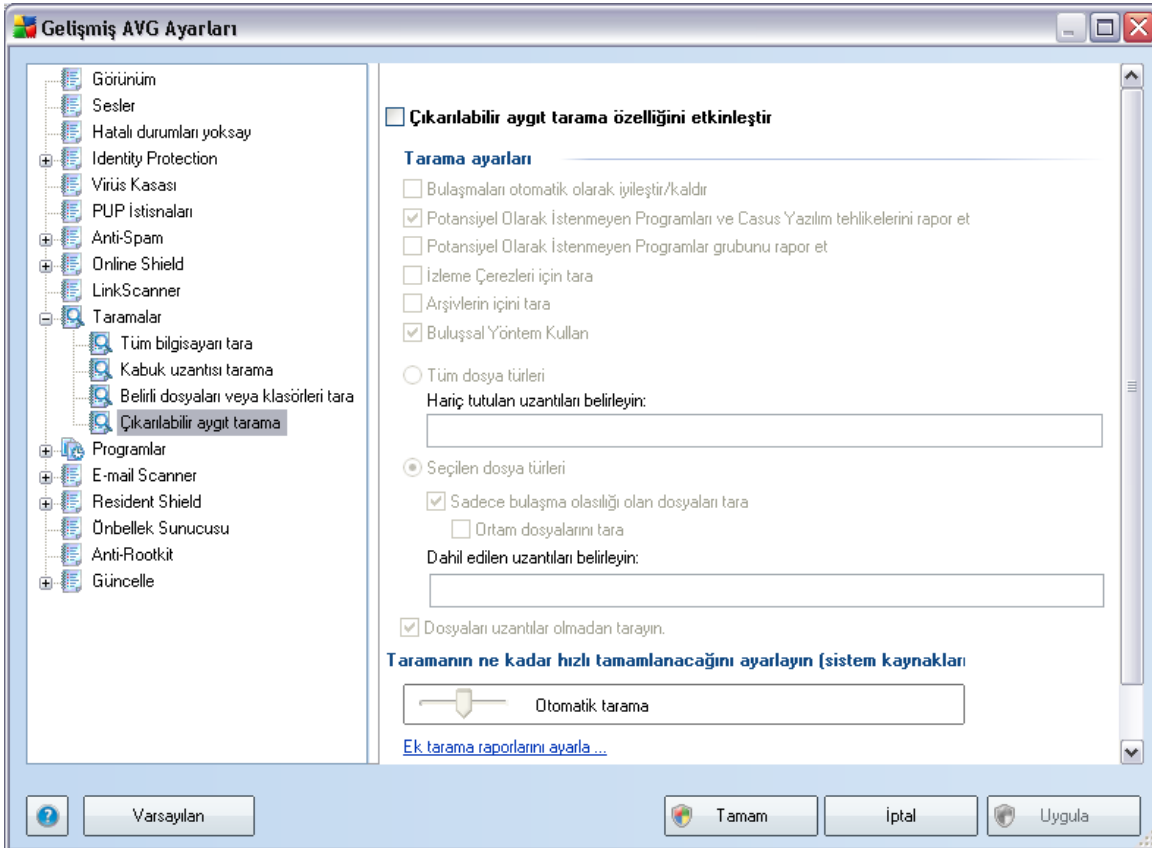


Bu yapılandırma iletişim kutusunda ayarlanan tüm parametreleri **Belirli dosya ya da klasörleri tara** ile tarama sırasında seçilen alanlar için geçerlidir!

Not: Belirli parametrelerin tanımlar hususunda bilgi almak için **AVG Gelismis Ayarlar / Taramalar / Tüm Bilgisayar Taraması** bölümünü inceleyin.

10.8.4. Çıkarılabilir Aygıt Tarama

Çıkarılabilir sürücü taraması'nin düzenleme arayüzü [Tüm Bilgisayar Taraması](#) düzenleme penceresine oldukça benzerdir:



Çıkarılabilir sürücü taraması bilgisayarınıza çıkarılabilir bir aygıt taktığınız anda otomatik olarak baslar. Öntanımlı olarak söz konusu tarama işlemi kapalıdır. Diğer bir yandan baslıca bulaşma kaynaklarından biri oldukları için söz konusu çıkarılabilir sürücülerin potansiyel tehditlere karşı taranması hayati önem taşımaktadır. Bu tarama özelliğinin istendiği zaman otomatik olarak baslatılacak şekilde hazır bulundurulması için **Çıkarılabilir aygıt taramasını etkinleştir** seçeneğini işaretleyin.

Not: Belirli parametrelerin tanımlar hususunda bilgi almak için [AVG Gelişmiş Ayarlar / Taramalar / Tüm Bilgisayar Taraması](#) bölümünü inceleyin.

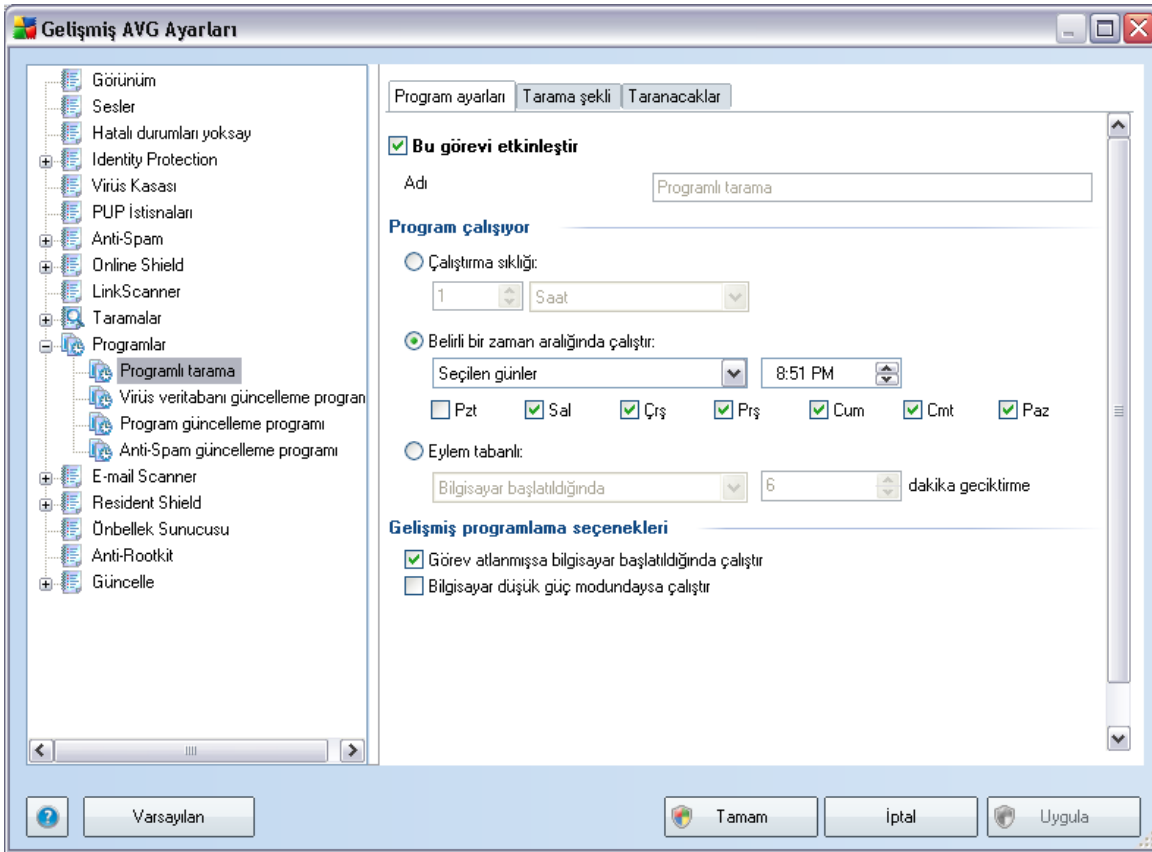
10.9. Programlar

Programlar bölümünde aşağıdaki bileşenlerin öntanımlı ayarlarını düzenleyebilirsiniz:

- [Tüm bilgisayar taraması programı](#)
- [Virüs veritabanı güncelleme programı](#)
- [Program güncelleme programı](#)

10.9.1. Programlı Tarama

Planlanan tarama parametreleri üç sekmeden düzenlenebilir: (*ya da yeni tarama planla*)



Planlama ayarları sekmesinde **Bu görevi etkinleştir** ögesini işaretleyerek ya da işareti kaldırarak planlanan taramayı geçici olarak devre dışı bırakabilir ve ihtiyaç duyduğunuzda yeniden açabilirsiniz.

Daha sonra, **Ad** adındaki metin alanında (*tüm varsayılan programlamalar için devre dışı bırakılmış*) bu programlamaya program satıcı tarafından atanan ad bulunur. Yeni eklenen zamanlamalar için (*sol gezinti ağacındayken **Taramayı programla** ögesi üzerinde sağ tıklayarak* yeni bir zamanlama ekleyebilirsiniz) kendi adınızı belirtebilirsiniz ve bu durumda metin alanı düzenleme için açılacaktır. Programladığınız taramaları diğerlerinden kolaylıkla ayırmak için her zaman taramalarınıza kısa, açıklayıcı adlar vermeye çalışın.

Örnek: Taramayı "Yeni Tarama" veya "Taramam" adıyla adlandırmanız uygun değildir çünkü bu adlar, taramanın fiilen neyi kontrol ettiğini açıklamaz. Diğer bir yandan "Sistem alanları taraması" oldukça açıklayıcı bir isim olacaktır. Ayrıca, taramanın adında söz konusu taramanın tam bilgisayar taraması ya da sadece seçilen dosya ya da klasörlerin taraması olup olmadığını belirtmenize gerek yoktur - taramalarınız [seçilen dosya ya da klasörleri tara](#) işlevinin farklı şekillerinden ibaret olacaktır.

Bu iletişim kutusunda taramanın aşağıdaki parametrelerini de tanımlayabilirsiniz:

Program çalışıyor

Burada, yeni programlanan tarama başlatması için zaman aralıkları belirtebilirsiniz. Zamanlama belirli bir sürenin ardından tekrarlanan tarama başlatması ile (**Her ...'de bir**) ya da kesin bir tarih ve saat tanımlayarak (**Belirli bir zaman aralığında çalıştır ...**) veya tarama başlangıcıyla ilgili bir olay tanımlanarak (**Bilgisayarın başlatılmasıyla ilişkili eylem**) tanımlanabilir.

Gelişmiş programlama seçenekleri

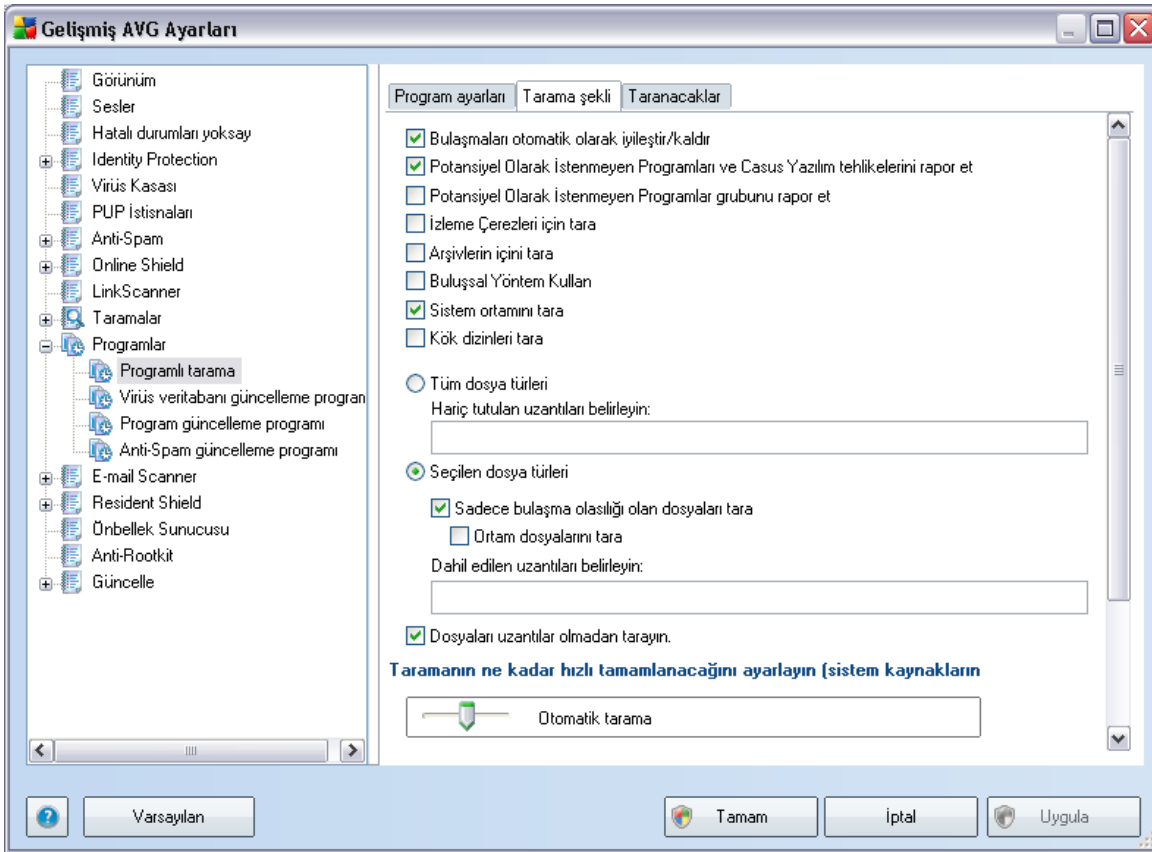
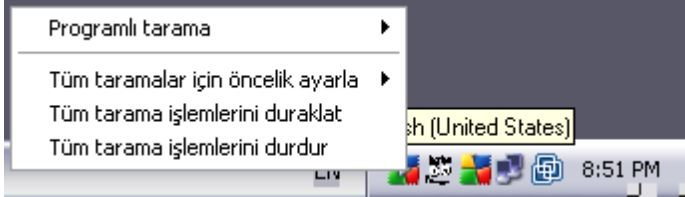
Bu bölümde, bilgisayar düşük güç modundaydı ya da tamamen kapatılmışsa hangi koşullar altında taramanın başlatılması/baslatılmaması gerektiğini tanımlamanızı sağlar.

Programlanan tarama belirttiğiniz saatte başlatıldığında, [AVG sistem tepsisi simgesi](#) üzerinde açılan bir açılır pencere ile bu konuda bilgilendirileceksiniz:





Bunun ardından [AVG sistem tepsisi simgesi](#) görüntülenir (üzerinde beyaz bir ok bulunur ve tamamen renklidir - yukarıdaki resme bakın) ve programlanan taramanın başladığını bildirir. Devam etmekte olan taramayı duraklatma ya da durdurma kararini verebileceğiniz bağlam menüsünü açmak için tarama devam ederken AVG simgesini sağ tıklayın:



Tarama Sekli sekmesinde, isteğe bağlı olarak açılıp/kapatılabilen tarama parametrelerine ilişkin bir liste bulabilirsiniz. Varsayılan olarak birçok parametre devreye sokulur ve

islevsellik de tarama sırasında uygulanacaktır. Söz konusu ayarları değiştirmek açısından geçerli bir nedeniniz yoksa öntanımlı konfigürasyonu olduğu gibi muhafaza etmeniz önerilir:

- **Bulasmayı otomatik temizle/sil** : tarama işlemi sırasında bir virüs tanımlanırsa ve temizlenmesi mümkün ise otomatik olarak temizlenir. Bulaşmış dosya otomatik olarak temizlenemezse, bulaşmış nesne [Virüs Kasası](#)'na taşınır.
- **Potansiyel Olarak İstenmeyen Programları ve Casus Yazılım tehlikelerini rapor et** - (varsayılan olarak açıktır): [Anti-Spyware](#) motorunu etkinleştirmek ve virüslerle birlikte casus yazılımları da kontrol etmek için isaretleyin. [Casus yazılım](#), kötü amaçlı yazılım olabilecek kategorisini temsil eder: bir güvenlik riski oluştursa da bu programlardan bazıları bilerek yüklenebilir. Bilgisayarınızın güvenliğini artırdığından, bu özelliği etkin durumda tutmanızı öneriyoruz.
- **Gelişmiş Potansiyel Olarak İstenmeyen Programlar setini bildir** - önceki seçenek etkinleştirilirse, genişletilmiş [casus yazılım](#) paketini algılamak için bu kutuyu da isaretleyebilirsiniz: doğrudan üreticiden alınan tamamen zararsız olan, ancak daha sonra kötüye kullanılan programlar. Bu, bilgisayar güvenliğinizi daha da artıran ek bir önlemdir, ancak yasal programları da engelleyebilir ve bu yüzden varsayılan olarak kapalıdır.
- **İzleme Tanımlama Bilgilerini Tara** - (varsayılan olarak açıktır): [Anti-Spyware](#) bileşeninin bu parametresi, tarama sırasında algılanılması istenen tanımlama bilgilerini tanımlar (*HTTP tanımlama bilgileri site tercihleri ya da elektronik alışveriş sepeti içeriği gibi kullanıcı hakkında belirli bilgilerin toplanması, temin edilmesi ve izlenmesi için kullanılır*)
- **Arsivleri Tara** - (varsayılan olarak açıktır): Bu parametreler, tarama işleminin ZIP, RAR gibi belirli bir arşiv türü ile sıkıştırılmış olsa bile tüm dosyaları taramasını öngörür.
- **Bulgusal Analiz Kullan** - (varsayılan olarak açıktır): bulgusal analiz (*taranan nesnenin sanal bir bilgisayar ortamında dinamik olarak canlandırılması'na ilişkin talimatlar*) tarama sırasında kullanılacak virüs tespiti yöntemlerinden birisidir;
- **Sistem ortamını tara** - (varsayılan olarak açıktır): tarama işlemi, bilgisayarınızın sistem alanlarını da kontrol edecektir;
- **Kök kullanıcıları tara** - Tam bilgisayar taraması yaparken kök kullanıcı tespitini de yapabilmek için bu öğeyi isaretleyin. Kök kullanıcı tespiti işlemini [Rootkit Önleme](#) bileşeninden de yapabilirsiniz;

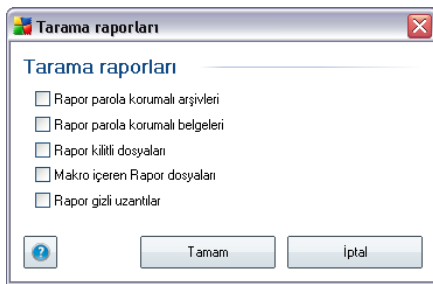
Ayrıca, taramak isteyip istemediğinize karar vermelisiniz

- **Tüm dosya türleri** , virgülle ayrılmış (*kaydedilirken virgüller noktalı virgüle dönüşür*) dosya uzantıları listesi sağlayarak taramadan hariç tutulacakların taranmaması için tanımlama olasıdır;
- **Seçili dosya türleri** - Yalnızca virüs bulasabilme olasılığı olan dosyaları taramayı istediğinizi belirtebilirsiniz (*virüs bulamayan dosyalar taranmayacaktır, örneğin, bazı düz metin dosyaları veya bazı diğer çalıştırılmayan dosyalar*); ortam dosyaları (*video, ses dosyaları - bu onay kutusunun işaretini kaldırırsanız, bu dosyalar genellikle çok büyük olduğundan ve virüs bulasma olasılıkları çok az olduğundan tarama süresini daha da azaltır*). Tekrar, her zaman taranması gereken dosyaları uzantılarına göre belirtebilirsiniz.
- İsteğe bağlı olarak, **Uzantıları olmayan dosyaları taramaya** da karar verebilirsiniz - bu seçenek varsayılan olarak açıktır ve gerçekten bir nedeniniz yoksa değiştirmeniz önerilir. Uzantısı olmayan dosyalar süpheli olabilir ve her zaman taranmalıdır.

Tarama işlemi önceliği

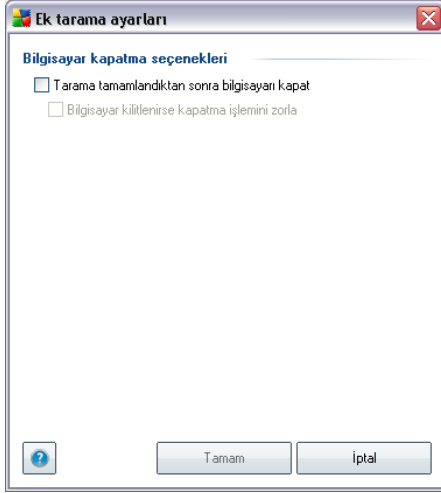
Tarama işlemi önceliği bölümünde, sistem kaynakları kullanımına bağlı olarak istediğiniz tarama hızını seçebilirsiniz. Varsayılan olarak bu seçenek, otomatik kaynak kullanımının ortalama düzeyine ayarlıdır. Tarama işleminin daha hızlı ilerlemesini istiyorsanız tarama işlemi daha kısa sürecektir fakat tarama işlemi sırasında sistem kaynakları oldukça yüklü bir şekilde kullanılacak ve bilgisayar üzerindeki diğer işlemleri yavaşlatacaktır (*bu seçenek bilgisayarınız açıkken kullanılmadığı sırada seçilebilir*). Öte yandan tarama süresini uzatarak da sistem kaynaklarının kullanımını azaltabilirsiniz.

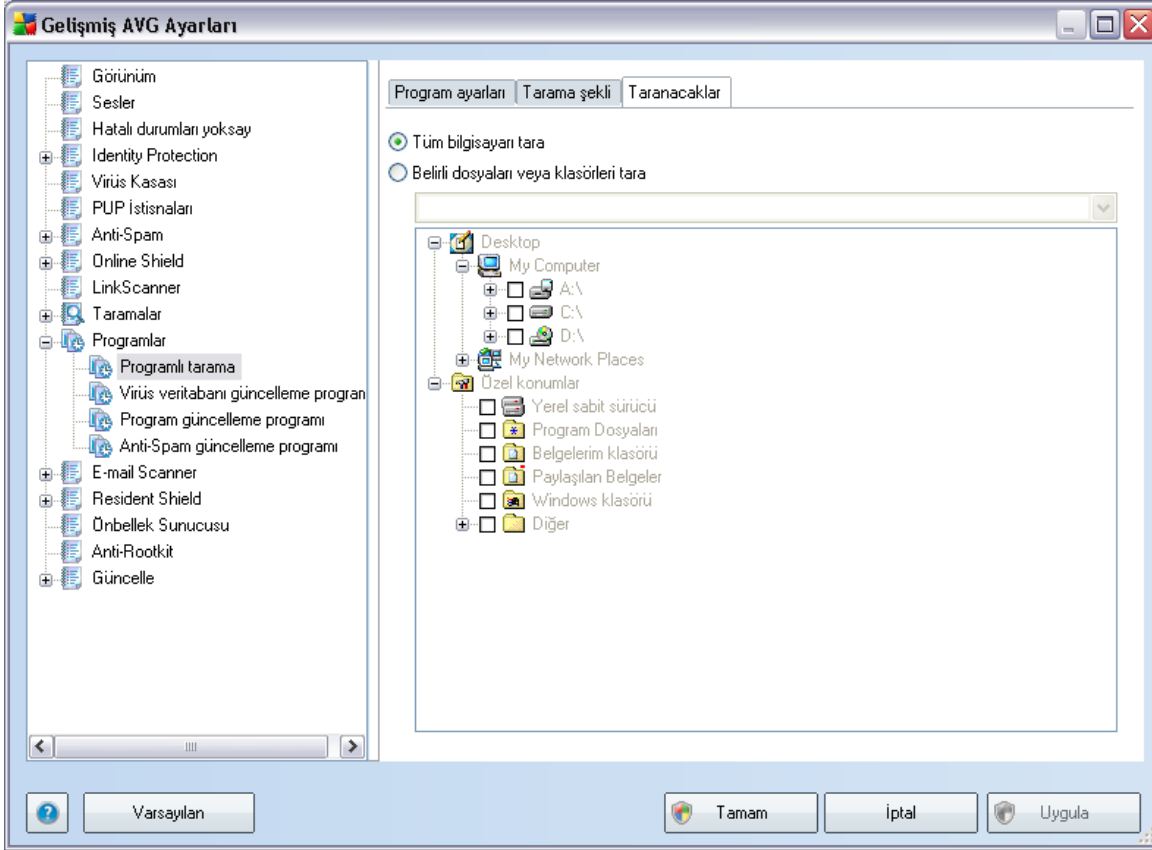
Diger tarama raporlarını belirle ... bağlantısına tıklayarak hangi tarama bulgularının rapor edileceğine ilişkin seçimleri yapabileceğiniz **Tarama raporları** iletişim kutusu penceresini açabilirsiniz:



Ekstra tarama ayarları'na tıklamak yeni bir **Bilgisayar Kapatma seçenekleri** iletişim kutusunu açar. Burada tarama işlemi bittikten sonra bilgisayarın otomatik olarak kapanmasını ayarlayabilirsiniz. Bu seçeneği seçerseniz (**Tarama bittikten sonra**

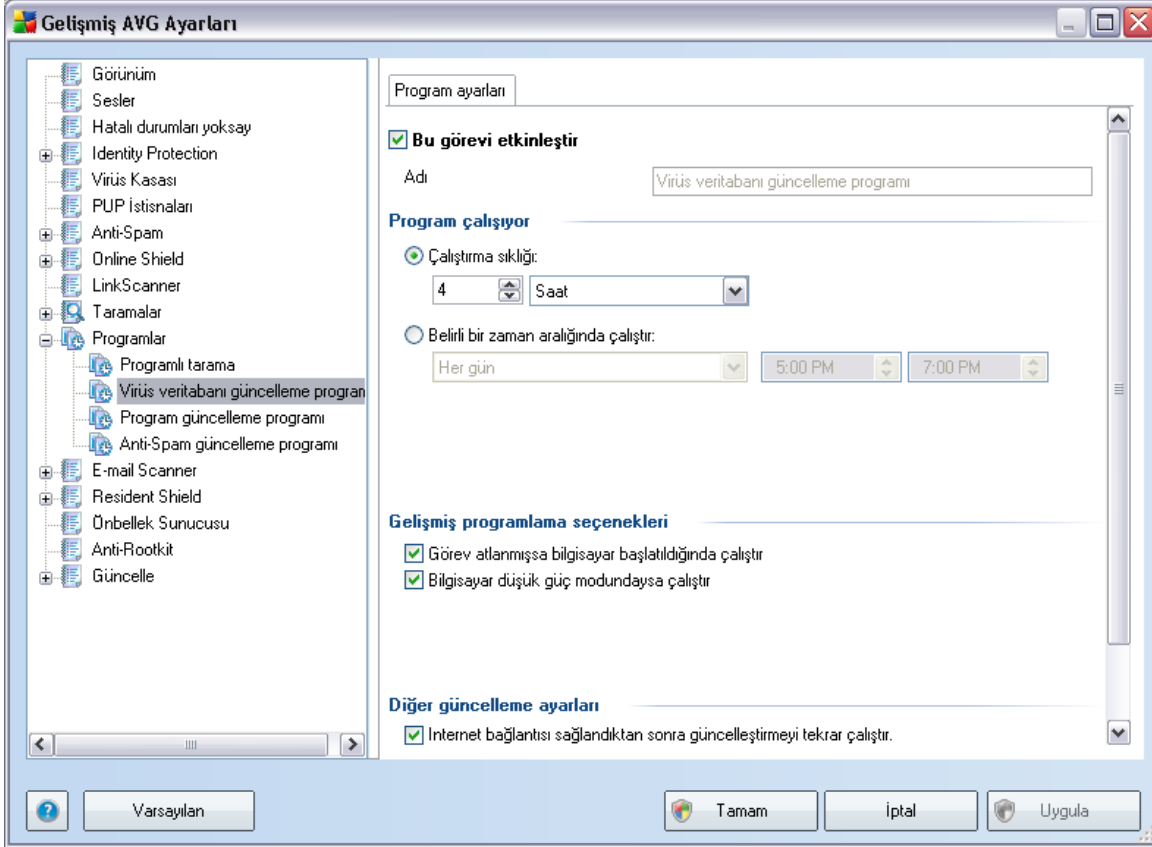
bilgisayari kapat)bilgisayar mevcut durumda kilitli olsa bile bilgisayarın kapatılmasını sağlayan bir seçeneğin bulunduğu bir pencere açılacaktır (**Bilgisayar kilitliyse bilgisayarın kapanmaya zorla**).





Taranacaklar sekmesinde, [tüm bilgisayarı tarama](#) veya [belirli dosya veya klasörleri taramayı](#) programlamak isteyip istemediğinizi belirleyebilirsiniz. Belirli dosya ve klasörleri taramayı seçerseniz, bu iletişim penceresinin alt kısmında görüntülenen ağaç yapısı etkinleşir ve taranacak klasörleri seçebilirsiniz.

10.9.2. Virüs Veritabanı Güncelleme Programı



Planlama ayarları sekmesinde **Bu görevi etkinleştir** ögesini işaretleyerek ya da işareti kaldırarak planlanan virüs veritabanı güncellemesini geçici olarak devre dışı bırakabilir ve ihtiyaç duyduğunuzda yeniden açabilirsiniz. Temel virüs veritabanı güncelleme programlama işlemi **Güncelleme Yöneticisi** bileşeni kapsamında açıklanmıştır. Bu iletişim kutusunda virüs veritabanı güncelleme planı parametrelerinden bazılarını ayrıntılarıyla yapılandırabilirsiniz. **Ad** adındaki metin alanında (*tüm varsayılan programlamalar için devre dışı bırakılmış*) bu programlamaya program satıcısı tarafından atanan ad bulunur.

Program çalışıyor

Bu bölümde, yeni programlanan virüs veritabanı güncellemesini başlatmak için zaman aralıkları belirtin. Zamanlama, belirli bir süreden sonra (**Çalıştırma sıklığı...**) tekrarlanan güncelleme başlatması olarak veya belirli bir tarih ve saat (**Belirli bir saatte çalıştır...**)



tanımlanarak tanımlanabilir.

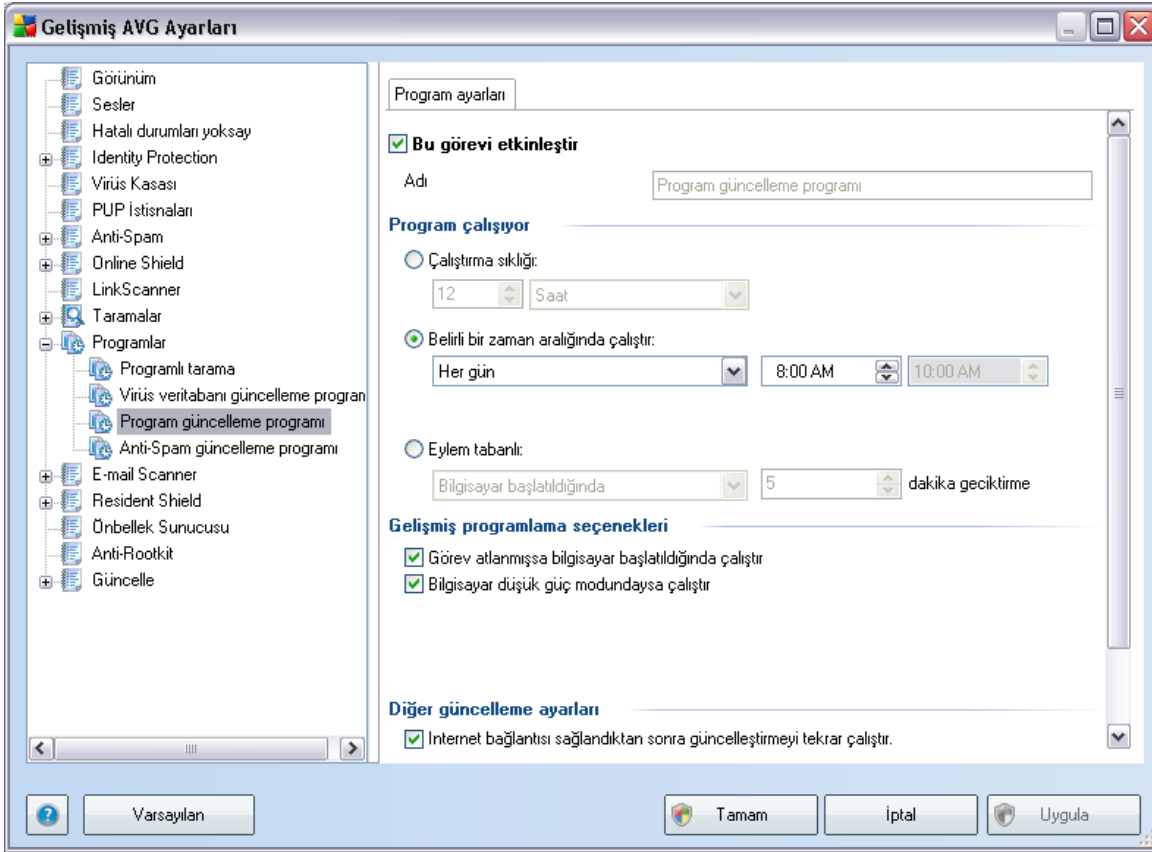
Gelismis programlama seçenekleri

Bu bölümde, bilgisayar düşük güç modundaydı veya tamamen kapatılmışsa hangi koşullar altında virüs veritabanı güncellemesinin başlatılması/baslatılmaması gerektiğini belirleyebilirsiniz.

Diğer güncelleme ayarları

Son olarak, ***Internet bağlantısı kurulduğunda güncellemeyi yeniden çalıştır*** seçeneğini işaretleyerek Internet bağlantısı bozulduğunda ve güncelleme işlemi başarısız olduğunda, Internet bağlantısı yeniden sağlanır sağlanmaz yeniden başlatıldığından emin olun.

Planlanan güncelleme işlemi sizin belirlediğiniz tarih ve saatte başladıktan sonra [AVG sistem tepsisi simgesi](#) üzerinde açılan bir açılır pencere vasıtasıyla bilgilendirileceksiniz (***Gelismis Ayarlar/Görünüm*** iletişim kutusunun varsayılan yapılandırmasını değiştirmemiş olmanız kaydıyla).



Planlama ayarları sekmesinde **Bu görevi etkinleştir** ögesini işaretleyerek ya da işareti kaldırarak planlanan güncellemesini geçici olarak devre dışı bırakabilir ve ihtiyaç duyduğunuzda yeniden açabilirsiniz. **Ad** adındaki metin alanında (*tüm varsayılan zamanlamalar için devre dışı bırakılmış*) bu zamanlamaya program satıcı tarafından atanan ad bulunur.

Program çalışıyor

Burada, yeni planlanan program güncellemesinin başlaması için zaman aralıklarını girin. Zamanlama belirli bir sürenin ardından tekrarlanan güncelleme ile (**Her ...'de bir**) ya da kesin bir tarih ve saat tanımlayarak (**Belirli bir saatte çalıştır ...**) ya da (**Bilgisayar başlangıcında**) ilgili bir programın güncellemesiyle tanımlanabilir.

Gelismis programlama seçenekleri

Bu bölümde, bilgisayar düşük güç modundaydı veya tamamen kapatılmışsa hangi koşullar altında program güncellemesinin başlatılması/baslatılmaması gerektiğini belirleyebilirsiniz.

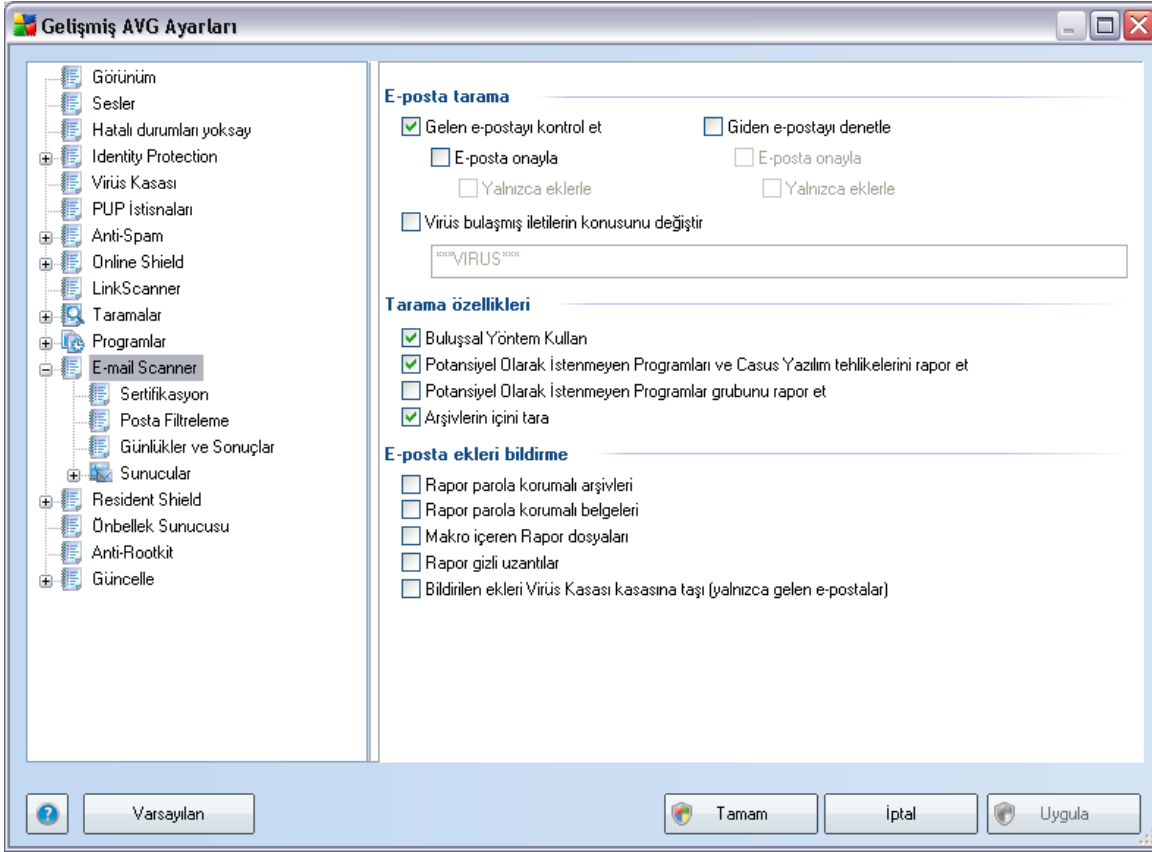
Diğer güncelleme ayarları

İnternet bağlantısı kurulduğunda güncellemeyi yeniden çalıştır seçeneğini işaretleyerek İnternet bağlantısı bozulduğunda ve güncelleme işlemi başarısız olduğunda, İnternet bağlantısı yeniden sağlanır sağlanmaz yeniden başlatıldığından emin olun.

Planlanan güncelleme işlemi sizin belirlediğiniz tarih ve saatte başladıktan sonra [AVG sistem tepsi simgesi](#) üzerinde açılan bir açılır pencere vasıtasıyla bilgilendirileceksiniz ([Gelismis Ayarlar/Görünüm](#) iletişim kutusunun varsayılan yapılandırmasını değiştirmemiş olmanız kaydıyla).

Not: Programlanmış bir program güncellemesinin zaman çakışması olursa ve programlanmış tarama gerçekleşirse, güncelleme işlemi yüksek önceliklidir ve tarama kesilir.

10.10. E-Posta Tarayıcısı



E-Posta Tarayıcısı iletişim kutusu üç bölüme ayrılmıştır:

- **E-posta tarama** - bu kısımda, gelen ve/veya giden e-posta iletileri için bu temel bilgileri ayarlayabilirsiniz:
 - o E-posta iletilerinin virüslere karşı taranıp taranmayacağı.
 - o Onay metninin, iletinin virüs içermediğini belirtmek üzere her iletinin sonuna eklenip eklenmeyeceği. Metin [Sertifikasyon](#) iletişim kutusunda ayarlanabilir.
 - o Onay metninin yalnızca ekli metinlere eklenip eklenmeyeceği.

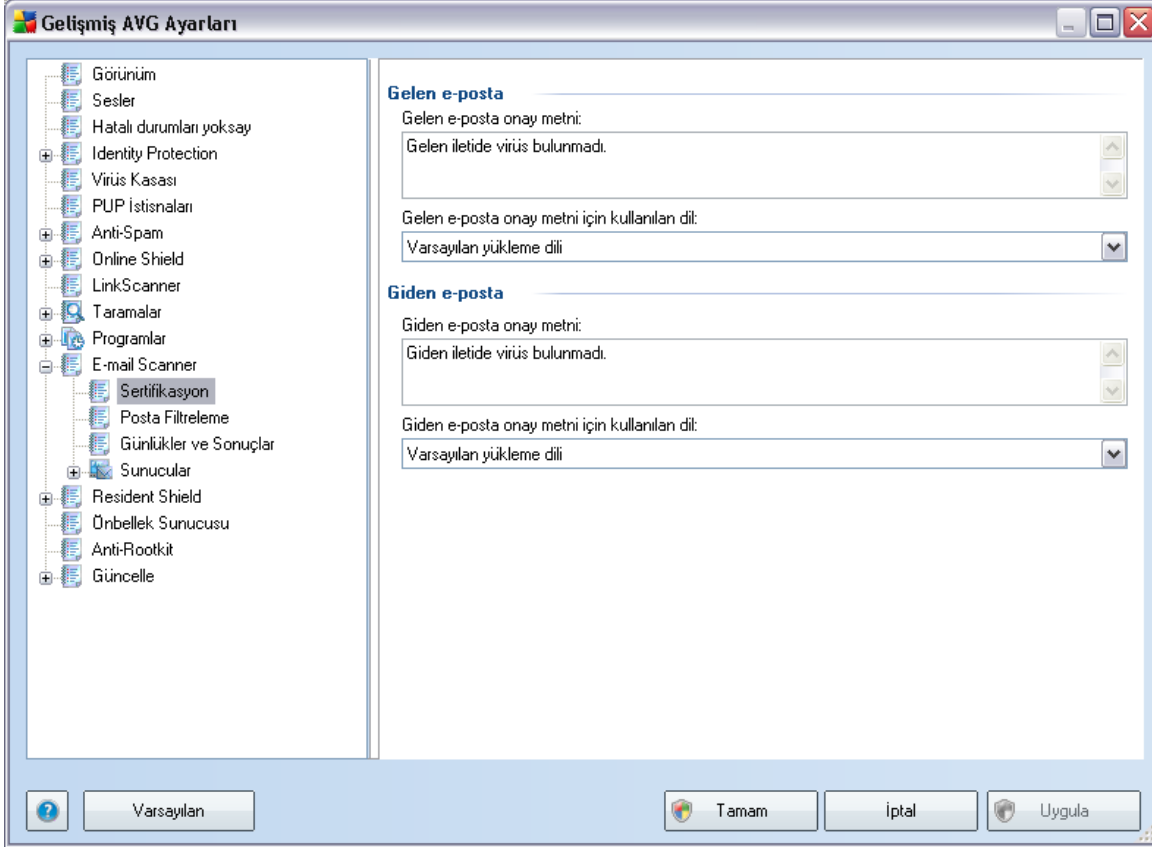
Virüs bulaşmış iletilerin konu satirini değiştirmek için, kutuyu işaretleyin ve istenen değeri metin alanına girin. Ardından, bu değeri, daha kolay tanımlanması

ve filtrelenmesi için bulaşan her e-posta iletişinin konu alanına girilecektir. Varsayılan değer ***VIRUS*** olarak belirlenmiştir ve bu değeri korumanızı öneririz.

- **Tarama özellikleri** - bu kısımda, e-posta iletilerinin nasıl taranacağını belirleyebilirsiniz:
 - o **Bulussal Yöntem Kullan** - e-posta iletilerini tararken [bulussal tespit yöntemi](#) kullanmak için işaretleyin. Bu seçenek açık olduğunda, e-posta eklerini yalnızca uzantıya göre filtreleyemezsiniz; ekin gerçek içeriği de göz önünde bulundurulur. Filtreleme işlemi [Posta Filtreleme](#) iletişim kutusundan ayarlanabilir.
 - o **Potansiyel Olarak İstenmeyen Programları ve Casus Yazılım tehlikelerini rapor et** - (varsayılan olarak açıktır): [Anti-Spyware](#) motorunu etkinleştirmek ve virüslerle birlikte casus yazılımları da kontrol etmek için işaretleyin. [Casus yazılım](#), kötü amaçlı yazılım olabilecek kategorisini temsil eder: bir güvenlik riski oluştursa da bu programlardan bazıları bilerek yüklenebilir. Bilgisayarınızın güvenliğini artırdığından, bu özelliği etkin durumda tutmanızı öneriyoruz.
 - o **Gelişmiş Potansiyel Olarak İstenmeyen Programlar setini bildir** - önceki seçenek etkinleştirilirse, genişletilmiş [casus yazılım](#) paketini algılamak için bu kutuyu da işaretleyebilirsiniz: doğrudan üreticiden alınan tamamen zararsız olan, ancak daha sonra kötüye kullanılan programlar. Bu, bilgisayar güvenliğinizi daha da artıran ek bir önlemdir, ancak yasal programları da engelleyebilir ve bu yüzden varsayılan olarak kapalıdır.
 - o **Arsivlerin içeriğini tara**: E-posta iletilerine eklenen arşivlerin içeriklerini taramak için işaretleyin.
- **E-posta ekleri bildirme** - bu kısımda, potansiyel olarak tehlikeli ve şüpheli olan dosyalar için ek raporlar ayarlayabilirsiniz. Lütfen bir uyarı iletişim kutusu görüntülenmeyeceğini unutmayın; yalnızca e-posta iletişinin sonuna bir onay metni eklenir ve bu tür tüm raporlar [E-posta Tarayıcısı tespiti](#) iletişim kutusunda listelenir:
 - o **Parola korumalı arşivleri bildir** - Parolayla korunan arşivlerin (ZIP, RAR, vb.) virüs için taranması mümkün değildir; bunların potansiyel olarak tehlikeli olduklarını rapor etmek için kutuyu işaretleyin.
 - o **Parola korumalı belgeleri bildir**: Parolayla korunan belgelerin virüs için taranması mümkün değildir; bunların potansiyel olarak tehlikeli olduklarını rapor etmek için kutuyu işaretleyin.

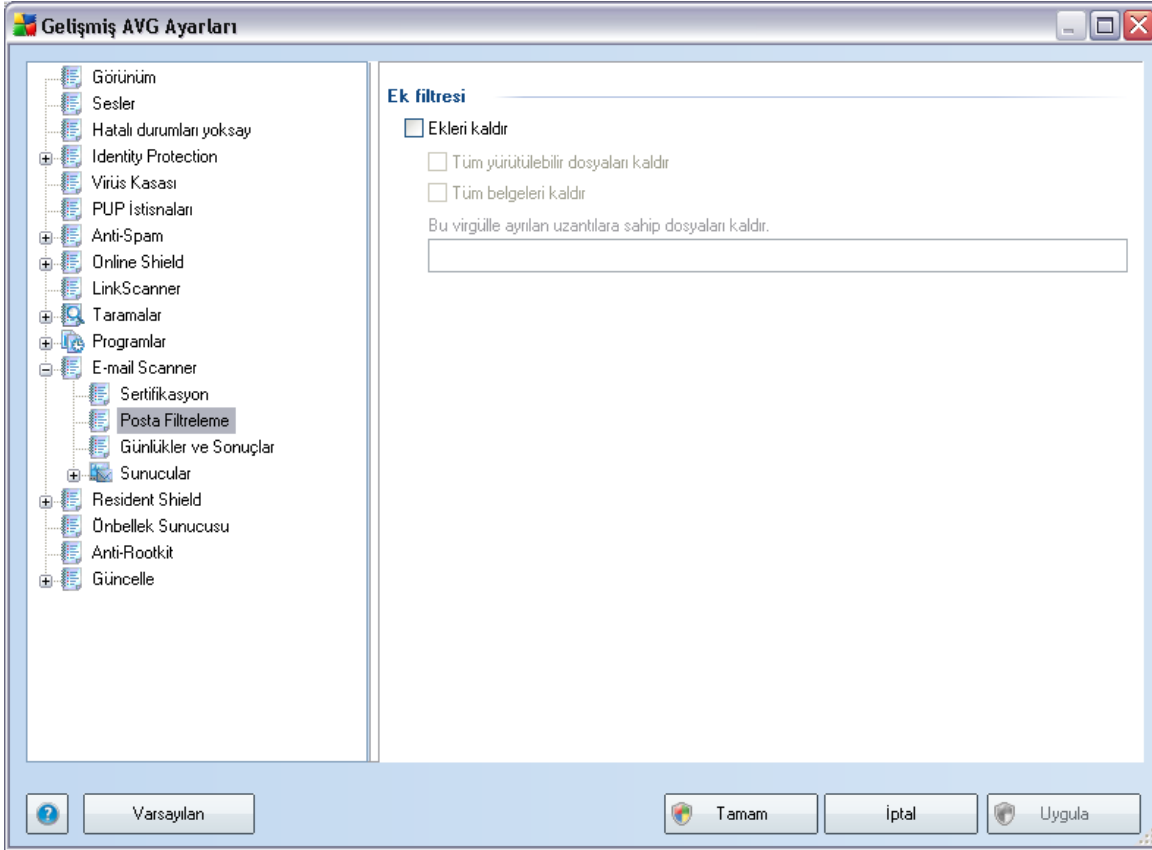
- o **Makro içeren dosyaları bildir:** Makro, bazı görevlerin kullanıcı için daha kolay hale getirilmesini amaçlayan önceden tanımlanmış adımlar dizisidir (MS Word makroları yaygın olarak tanınır). Makro, potansiyel olarak tehlikeli talimatlar içerebilir ve makro içeren dosyaların şüpheli olarak rapor edilmesini sağlamak için kutuyu işaretleyebilirsiniz.
- o **Gizlenen uzantıları bildir** - Gizli uzantılar şüpheli bir çalıştırılabilir dosyayı (örn. "birsey.txt.exe") zararsız bir düz metin dosyası gibi (örn. "birsey.txt") gösterebilir; bunları potansiyel olarak tehlikeli olarak rapor etmek için kutuyu işaretleyin.
- o **Rapor edilen ekleri Virüs Kasasına taşı** - taranan e-posta iletişimin ekinde gizli bir eklenti tespit edildiğinde parola korumalı arşivler, parola korumalı belgeler, makro içeren belgeler ve/veya dosyalar hakkında e-posta vasıtasıyla bilgilendirilmek isteyip istemediğinizi belirtin. Tarama işlemi sırasında bu tür bir mesaj tespit edilirse tespit edilen bulasmış nesnenin [Virüs Kasasına](#) taşınmasını isteyip istemediğinizi belirtin.

10.10.1. Sertifikasyon



Sertifikalar iletişim kutusunda sertifika bildiriminde gösterilecek metni ve dili seçebilirsiniz. Bu ayar **Gelen posta** ve **Giden posta için ayrı ayrı yapılmalıdır**.

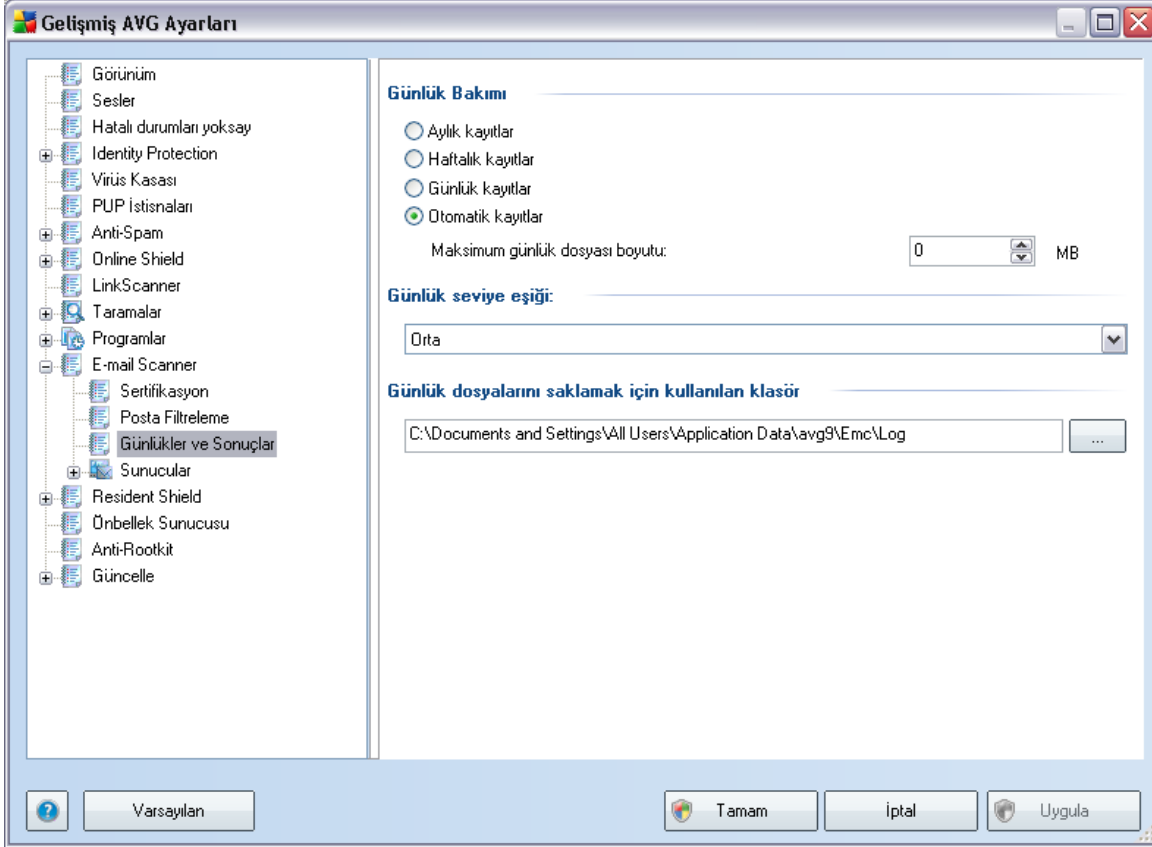
10.10.2. Posta Filtreleme



Ek filtresi iletişim kutusu, e-posta mesajlarının eklerinin taranmasına ilişkin parametreleri ayarlayabilmenizi sağlar. Varsayılan olarak **Eklentileri sil** seçeneği kapalıdır. Etkinleştirmeye karar vererseniz tüm e-posta mesajlarının eklentileri, bulaşmış nesne ya da potansiyel olarak tehlikeli nesne olarak algılanacak ve silinecektir. Belirli ek türlerinin silinmesini istiyorsanız ilgili seçeneği seçin:

- **Tüm çalıştırılabilir dosyaları sil** - tüm *.exe dosyaları silinecektir
- **Tüm belgeleri kaldır** - tüm *.doc, *.docx, *.xls, *.xlsx dosyaları silinecektir
- **Virgülle ayrılmış su uzantılara sahip dosyaları kaldır** - Tanımlanan uzantılara sahip tüm dosyalar kaldırılacaktır

10.10.3. Günlükler ve Sonuçlar

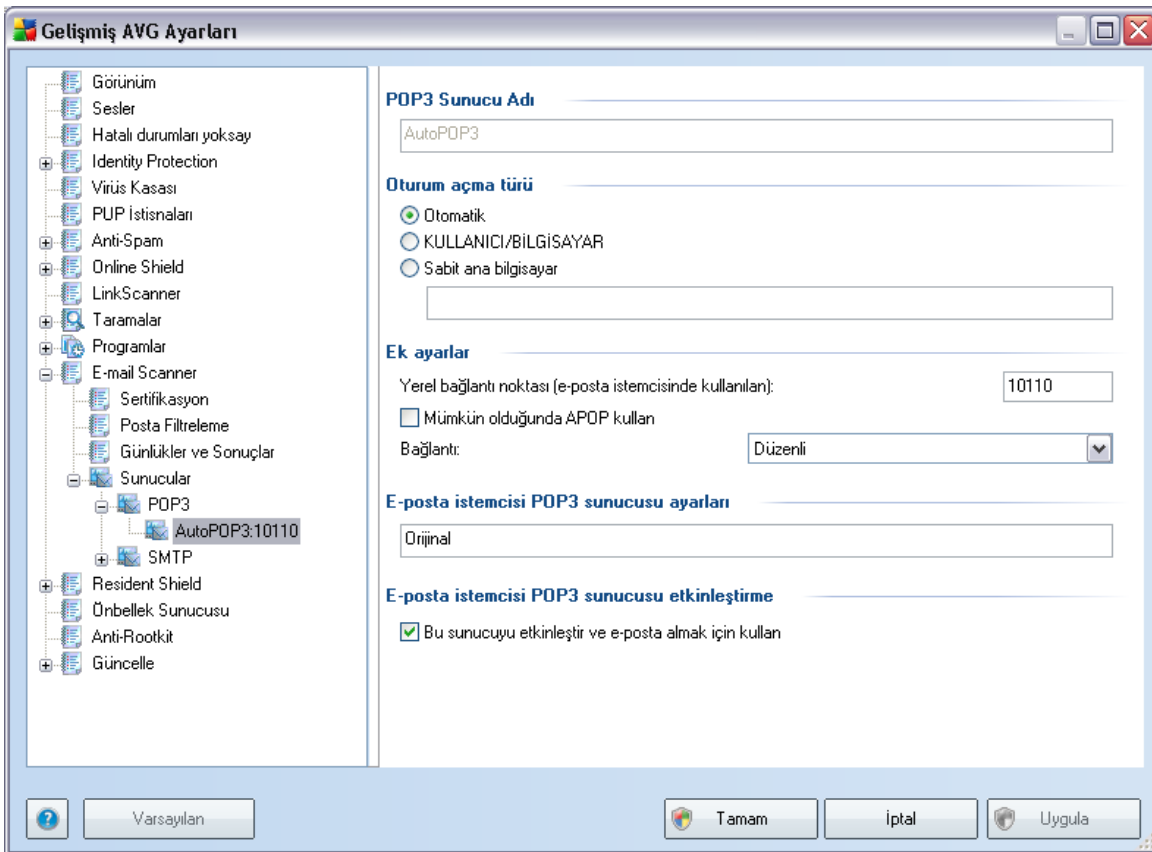


Kayıt ve Sonuçlar dolasim ögesinden açılan iletişim penceresi, e-posta tarama sonuçlarının bakım parametrelerini belirlemenizi sağlar. İletişim penceresi çok sayıda bölüme ayrılır:

- **Kayıt Defteri Bakımı** - e-posta tarama bilgilerinin günlük, haftalık ya da aylık olarak kaydedilmesini isteyip istemediğini belirleyin; buna ek olarak kayıt dosyasının maksimum boyutunu (*MB cinsinden*) girin.
- **Kayıt Seviyesi Esigi** - öntanımlı olarak orta seviyeye ayarlanmıştır - daha düşük bir seviye (*sadece baslıca bağlantı bilgilerinin kaydı tutulur*) ya da daha yüksek bir seviye (*tüm trafik bilgileri kaydedilir*) seçebilirsiniz.
- **Kayıt dosyalarını kaydetmek için kullanılacak dosya** - kayıt dosyasının nerece kaydedileceğini belirleyin

10.10.4. Sunucular

Sunucular bölümünde **E-posta Tarayicisi** bileşeninin sunucu parametrelerini değiştirebilir ya da **Yeni sunucu ekle** düğmesini kullanarak yeni sunucu yapılandırabilirsiniz.

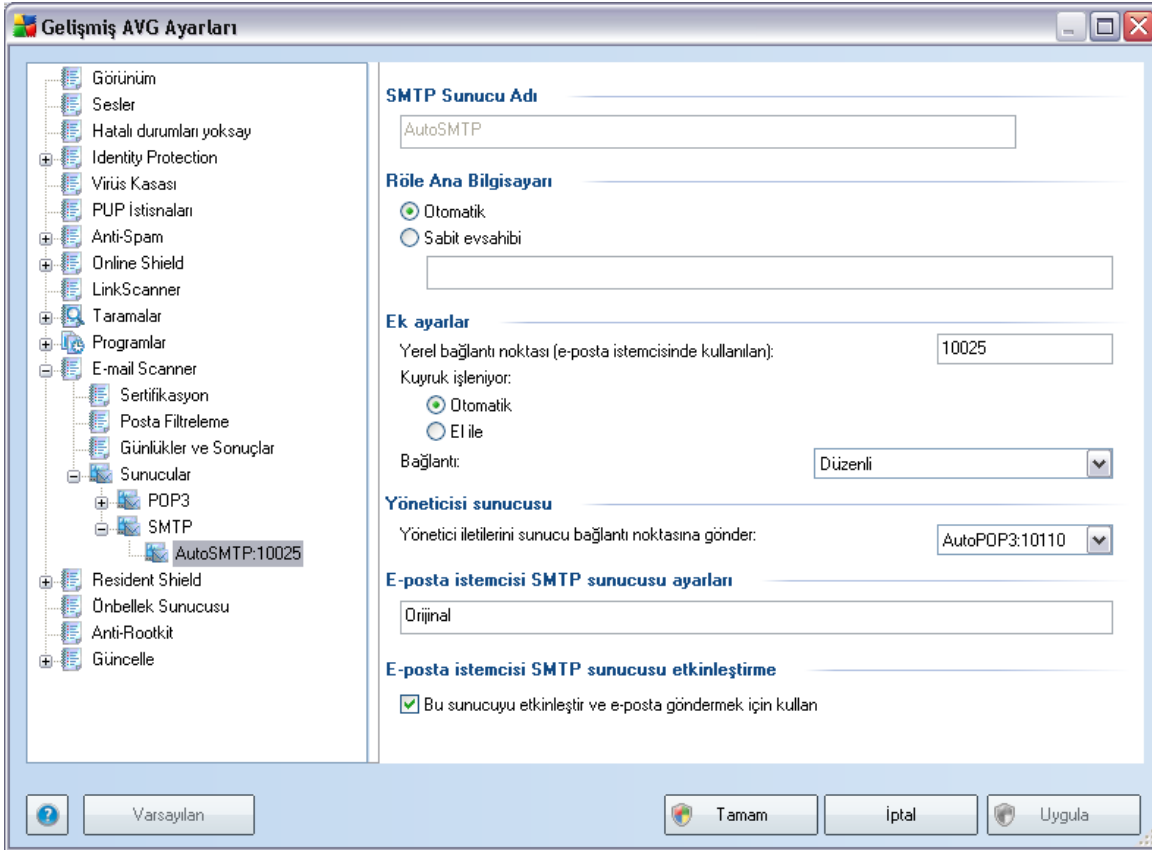


Bu iletişim kutusunda (**Sunucular / POP3 üzerinden açılır**) yeni bir **E-posta Tarayicisi** sunucusu belirlemek üzere gelen postalar için POP3 protokolünü kullanabilirsiniz:

- **POP3 Sunucusu Adı** - sunucunun adının yerine yazın ya da AutoPOP3 şeklindeki varsayılan adı muhafaza edin
- **Oturum açma tipi** - gelen postalar için kullanılan posta sunucularının belirlenmesi sırasında kullanılan yöntemi tanımlar:

- o **Otomatik** - Oturum açma işlemi, e-posta istemcinizin ayarlarına göre otomatik olarak gerçekleştirilir.
- o **KULLANICI/BILGISAYAR** - Hedef posta sunucusunu tanımlamak için en kolay ve en sık kullanılan yöntem proxy yöntemidir. Bu yöntemi kullanmak için, ilgili posta sunucusuna ilişkin oturum açma kullanıcı adının bir bölümü olarak ad veya adresi / karakteriyle ayırarak belirtin. Örneğin; pop.acme.com sunucusunda ve bağlantı noktası 8200'deki kullanıcı1 hesabi söz konusu olduğunda oturum açma adı olarak kullanıcı1/pop.acme.com:8200 kullanabilirsiniz.
- o **Sabit ana bilgisayar** - Bu durumda, program her zaman burada belirtilen sunucuyu kullanır. Lütfen posta sunucunuzun adresini veya adını belirtin. Oturum açma adı değişmez. Ad için, etki alanı adı (örn. pop.acme.com) ve IP adresi (123.45.67.89) kullanabilirsiniz. Posta sunucusu standart olmayan bir bağlantı noktası kullanıyorsa, bu bağlantı noktasını ayırıcı olarak iki nokta üst üste kullanarak sunucu adının arkasına girebilirsiniz (örn. smtp.acme.com:8200). POP3 iletişimi için varsayılan bağlantı noktası 110'dur.
- **Diger ayarlar** - daha ayrıntılı parametreleri belirler:
 - o **Yerel bağlantı noktası** - Posta uygulamanızın iletişim kurması beklenen bağlantı noktasını belirler. Posta uygulamanızda, bu bağlantı noktasını POP3 iletişimi bağlantı noktası olarak belirtmeniz gerekir.
 - o **Mevcut ise APOP kullan** - Bu seçenek, posta sunucularında daha güvenilir oturum açabilmenizi sağlar. Bu, **E-posta Tarayicisinin** kullanıcı hesabi parolasını göndermek için başka bir yöntem kullanmasını ve sunucudan alınan değişken zinciri kullanarak parolayı sunucuya şifrelenmiş biçimde göndermesini sağlar. Doğal olarak bu özellik, yalnızca hedef posta sunucusu tarafından desteklendiginde kullanılabilir.
 - o **Baglanti** - Açılır menüden kullanılacak bağlantı türünü seçebilirsiniz (normal/SSL/SSL varsayılan). SSL bağlantıyı tercih ederseniz, gönderilen veri, üçüncü bir taraf tarafından izlenme riski olmayacak şekilde şifrelenir. Bu özellik de, yalnızca hedef posta sunucusu tarafından desteklendiginde kullanılabilir.
- **E-posta istemcisi POP3 sunucusu ayarları** - e-posta istemcinizi düzgün şekilde yapılandırmanız için gerekli olan yapılandırma (böylece, **E-posta Tarayicisi** tüm gelen postaları tarar) hakkında kısa bir bilgi sağlar. Bu, söz konusu iletişim kutusunda ve diğer iletişim kutularında belirtilen ilgili parametreleri temel alan bir özetdir.

- **E-posta istemcisi POP3 sunucusu etkinleştirme** - Belirtilen POP3 sunucusunu etkinleştirmek veya devre dışı bırakmak için bu öğeyi isaretleyin/ isaretini kaldırın.



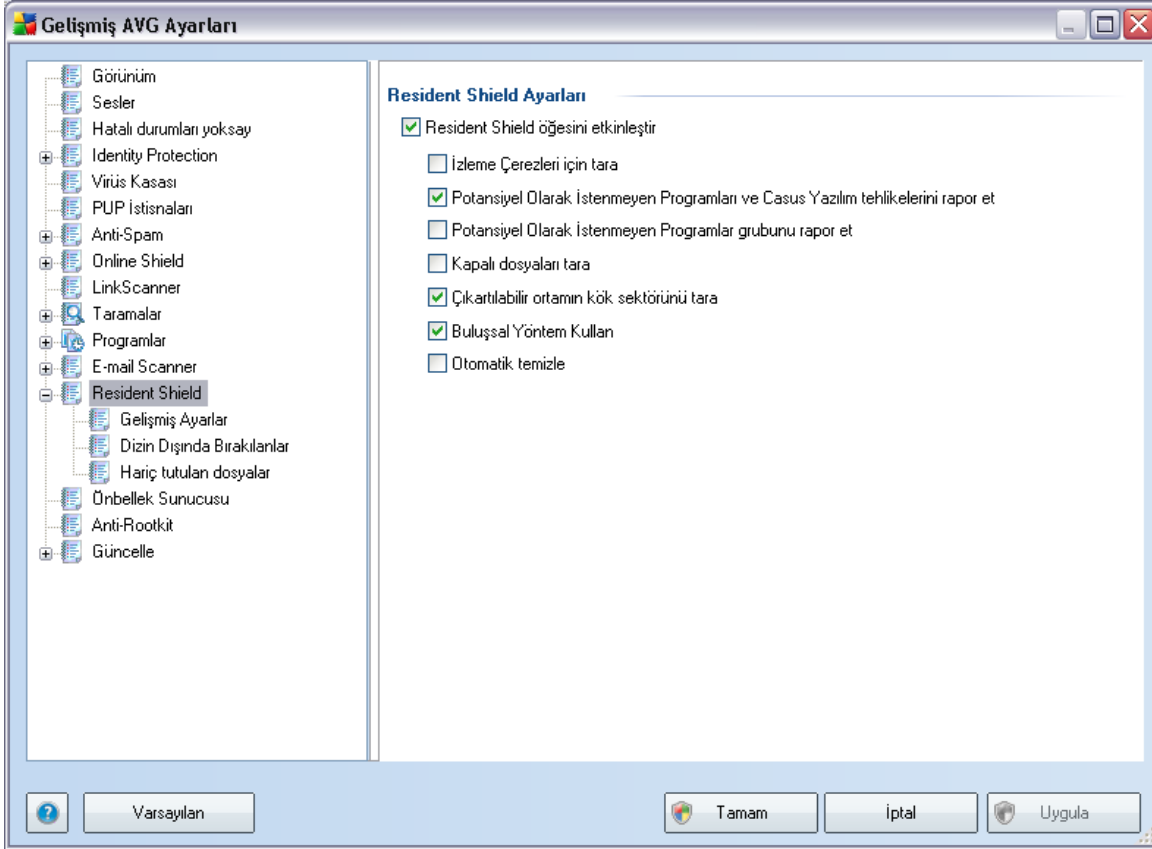
Bu iletişim kutusunda (**Sunucular /SMTP üzerinden açılır**) yeni bir **E-posta Tarayıcısı** sunucusu belirlemek üzere giden postalar için SMTP protokolünü kullanabilirsiniz:

- **SMTP Sunucusu Adı** - sunucunun adının yerine yazın ya da AutoSMTP şeklindeki varsayılan adı muhafaza edin
- **Röle Ana Bilgisayarı** - giden postalar için kullanılan posta sunucularını tanımlama yöntemidir:
 - o **Otomatik** - Oturum açma işlemi, e-posta istemcinizin ayarlarına göre otomatik olarak gerçekleştirilir

- o **Sabit ana bilgisayar** - Bu durumda, program her zaman burada belirtilen sunucuyu kullanır. Lütfen posta sunucunuzun adresini veya adını belirtin. Ad için, etki alanı adı (örneğin, smtp.acme.com) ve IP adresi (örneğin, 123.45.67.89) kullanabilirsiniz. Posta sunucusu standart olmayan bir bağlantı noktası kullanıyorsa, bu bağlantı noktasını ayırıcı olarak iki nokta üst üste kullanarak sunucu adının arkasına girebilirsiniz (örn. smtp.acme.com:8200). SMTP iletişimi için standart bağlantı noktası 25'tir.
- **Diger ayarlar** - daha ayrıntılı parametreleri belirler:
 - o **Yerel bağlantı noktası** - Posta uygulamanızın iletişim kurması beklenen bağlantı noktasını belirler. Posta uygulamanızda, bu bağlantı noktasını SMTP iletişimi bağlantı noktası olarak belirtmeniz gerekir.
 - o **Sıra işlemi** - Posta mesajları gönderilirken gereksinimlerin işlenmesi sırasında **E-posta Tarayicisinin** davranışını belirler:
 - Otomatik: Giden posta anında hedef posta sunucusuna teslim edilir (gönderilir).
 - El ile: İlet, giden iletiler kuyruğuna eklenir ve daha sonra gönderilir
 - o **Baglanti** - Bu açılır menüden kullanılacak bağlantı türünü belirtebilirsiniz (normal/SSL/SSL varsayılan). SSL bağlantıyı tercih ederseniz, gönderilen veri, üçüncü bir taraf tarafından izlenme riski olmayacak şekilde şifrelenir. Bu özellik, yalnızca hedef posta sunucusu tarafından desteklendiğinde kullanılabilir.
- Yönetici sunucusu bölümü, yönetim raporlarının ters yöne gönderilmesi için kullanılan sunucu bağlantı noktası sayısını gösterir. Bu iletiler, örneğin hedef posta sunucusu giden mesajı reddettiğinde veya bu posta sunucusu kullanılabilir olmadığında oluşturulur.
- E-posta istemcisi SMTP sunucusu ayarları bölümü, istemci posta uygulamasının, giden iletilerin, E-posta Tarayicisinden gönderilen postaları kontrol etmek üzere kaydedilen sunucu kullanılarak kontrol edilmesini sağlayacak şekilde yapılandırılmasına ilişkin hızlı bilgiler sağlar. Bu, söz konusu iletişim kutusunda ve diğer iletişim kutularında belirtilen ilgili parametreleri temel alan bir özettir.
- **E-posta istemcisi SMTP sunucusu aktivasyonu** - yukarıda belirtilen SMTP sunucusunu etkinleştirmek/devre dışı bırakmak için bu kutuyu işaretleyin/ işaretini kaldırın

10.11. Yerleşik Kalkan

Yerleşik Kalkan bileşeni, dosya ve klasörlerinizi çevrimiçi ortamda virüslere, casus yazılımlar ve diğer zararlı yazılımlara karşı korur.



Yerleşik Kalkan Ayarları iletişim kutusunda **Yerleşik Kalkan** korumasını **Yerleşik Kalkanı Etkinleştir** ögesini işaretleyerek ya da işaretini kaldırarak etkinleştirebilir ya da devre dışı bırakabilirsiniz (*bu seçenek varsayılan olarak açıktır*). Buna ek olarak **Yerleşik Kalkan** hangi özelliklerinin etkinleştirileceğini de seçebilirsiniz.

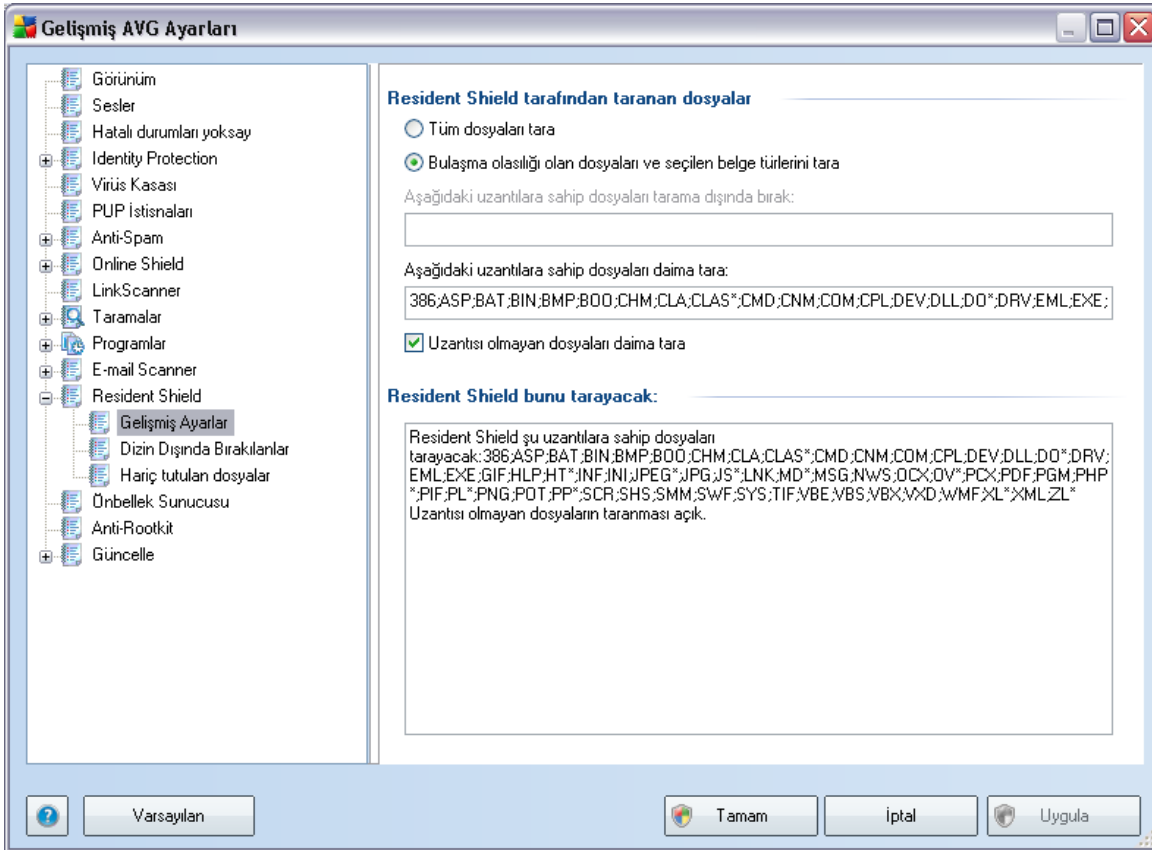
- **Tanımlama bilgilerini izlemek için tara** - bu parametre, tanımlama bilgilerinin tarama işlemi sırasında tespit edilmesi gerektiğini belirtir. (*HTTP tanımlama bilgileri, site tercihleri veya elektronik alışveriş sepetlerinin içerikleri gibi kullanıcılar hakkındaki belirli bilgilerin kimliklerinin doğrulanması, takibi ve sürdürülmesi için kullanılır.*)
- **Potansiyel Olarak İstenmeyen Programları ve Casus Yazılım tehlikelerini**

rapor et - (varsayılan olarak açıktır): [Anti-Spyware](#) motorunu etkinleştirmek ve virüslerle birlikte casus yazılımları da kontrol etmek için isaretleyin. [Casus yazılım](#), kötü amaçlı yazılım olabilecek kategorisini temsil eder: bir güvenlik riski oluştursa da bu programlardan bazıları bilerek yüklenebilir. Bilgisayarınızın güvenliğini artırdığından, bu özelliği etkin durumda tutmanızı öneriyoruz.

- **Gelişmiş Potansiyel Olarak İstenmeyen Programlar setini bildir** - önceki seçenek etkinleştirilirse, genişletilmiş [casus yazılım](#) paketini algılamak için bu kutuyu da isaretleyebilirsiniz: doğrudan üreticiden alınan tamamen zararsız olan, ancak daha sonra kötüye kullanılan programlar. Bu, bilgisayar güvenliğinizi daha da artıran ek bir önlemdir, ancak yasal programları da engelleyebilir ve bu yüzden varsayılan olarak kapalıdır.
- **İşlem sonunda tara** - işlem sonunda tarama, AVG'nin etkin nesneleri hem açılırken hem de kapatılırken taradığından emin olmanızı sağlar. Bunun yanı sıra bu özellik, bilgisayarınızı karmaşık virüslere karşı korumanıza da yardımcı olur
- **Çıkarılabilir ortamların önyükleme kesimini tara** - (varsayılan olarak açıktır)
- **Bulgusal Analiz Kullan** - (varsayılan olarak açıktır) [bulgusal analiz](#), tespit etme işlemi sırasında kullanılır(*taranan nesne'nin komutlarının sanal bilgisayar ortamında dinamik olarak canlandırılması*)
- **Otomatik Temizle** - tespit edilen bulasmalar, temizleme yöntemi mevcut ise otomatik olarak temizlenir.

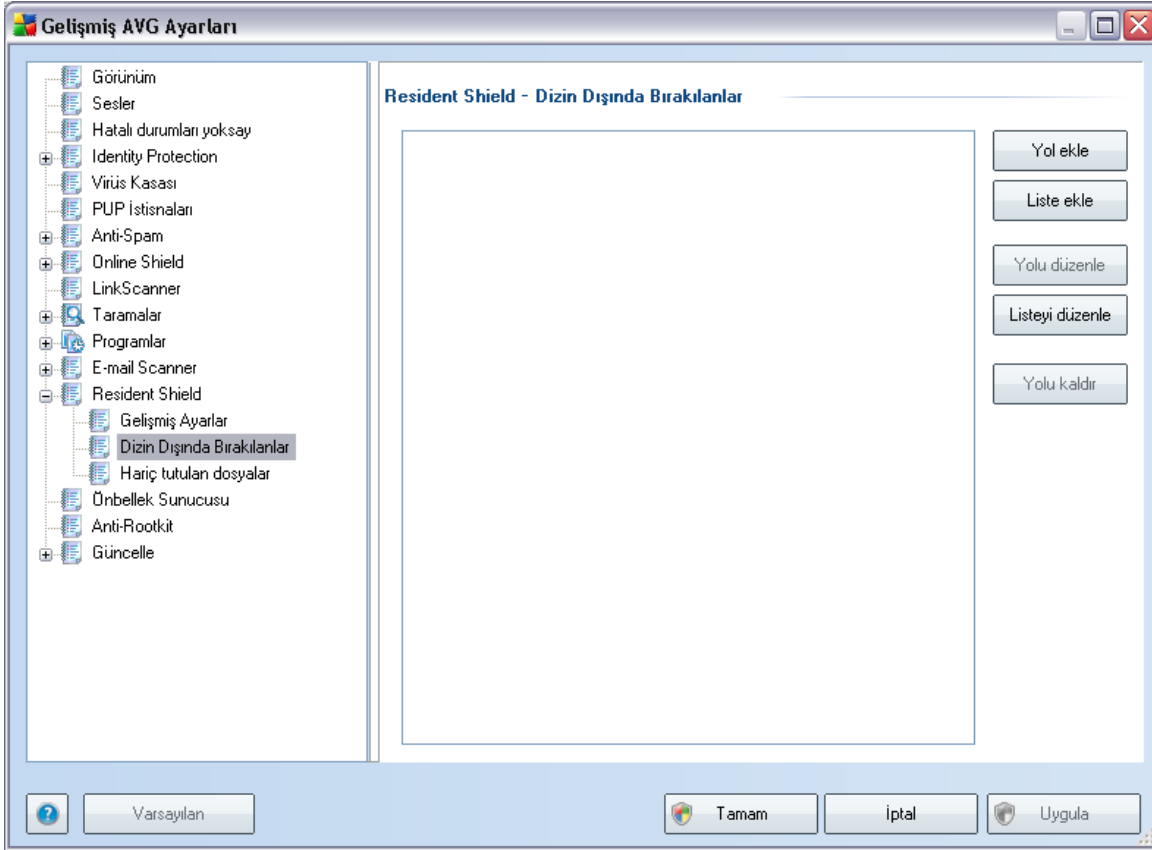
10.11.1. Gelişmiş Ayarlar

Yerlesik Kalkan tarafından taranan dosyalar penceresinde taranan dosyaların yapılandırılması mümkündür (*belirli dosya uzantılarına göre*):



Tüm dosyaların mı yoksa sadece bulmuş dosyaların mı taranacağına karar verin - Bunun ardından tarama işlemi sırasında hariç tutulacak dosyaları tanımlayan dosya uzantısı listesini de seçebilir, bunun yanı sıra her ne şart altında olursa olsun taranmasını istediğiniz dosyaları tanımlayan dosya uzantılarını gösteren bir liste de oluşturabilirsiniz.

10.11.2. Hariç Tutulan Dizin



Yerlesik Kalkan - İstisnalar Dizini iletişim kutusu [Yerlesik Kalkan](#) taraması sırasında hariç tutulacak klasörleri seçebilmenizi sağlar.

Gerekli değildir dolayısıyla izinlerin tarama işleminden çıkartılmasını kesinlikle önermiyoruz!

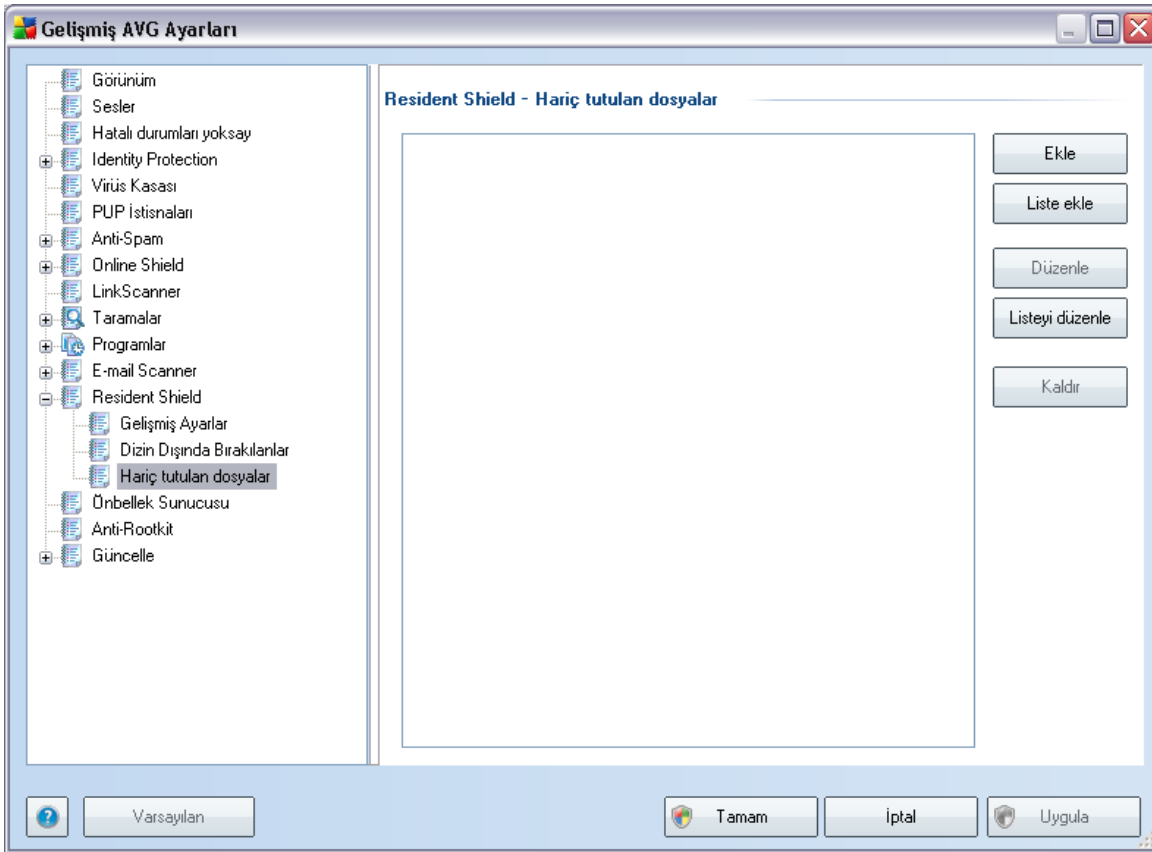
İletişim kutusunda aşağıdaki kontrol düğmeleri bulunur:

- **Veriyolu ekle**– yerel diskin dolayım ağacından teker teker seçmek suretiyle tarama işleminden hariç tutulacak izinleri belirleyin.
- **Liste ekle**– [Yerlesik Kalkan](#) taramasından hariç tutulacak izinlere ilişkin tam bir liste hazırlayabilmenizi sağlar
- **Veriyolunu düzenle**– seçilen klasöre giden veriyolunu düzenleyebilmenizi

saglar.

- **Listeyi düzenle**– klasör listesini düzenleyebilmenizi saglar.
- **Veriyolunu sil**– listeden seçilen klasöre giden yolu silebilmenizi saglar.

10.11.3. Hariç Tutulan Dosyalar



Yerlesik Kalkan - Hariç tutulan dosyalar iletisim kutusu önceden tanımlanan **Yerlesik Kalkan - Hariç Tutulan Dizin** olarak davranır, ancak klasörler yerine şimdi **Yerlesik Kalkan** taramasından hariç tutulacak belirli dosyaları tanımlayabilirsiniz.

Gerekmiyorsa, dosyaların hariç tutulmasını kesinlikle önermiyoruz!

İletisim kutusunda aşağıdaki kontrol düğmeleri bulunur:

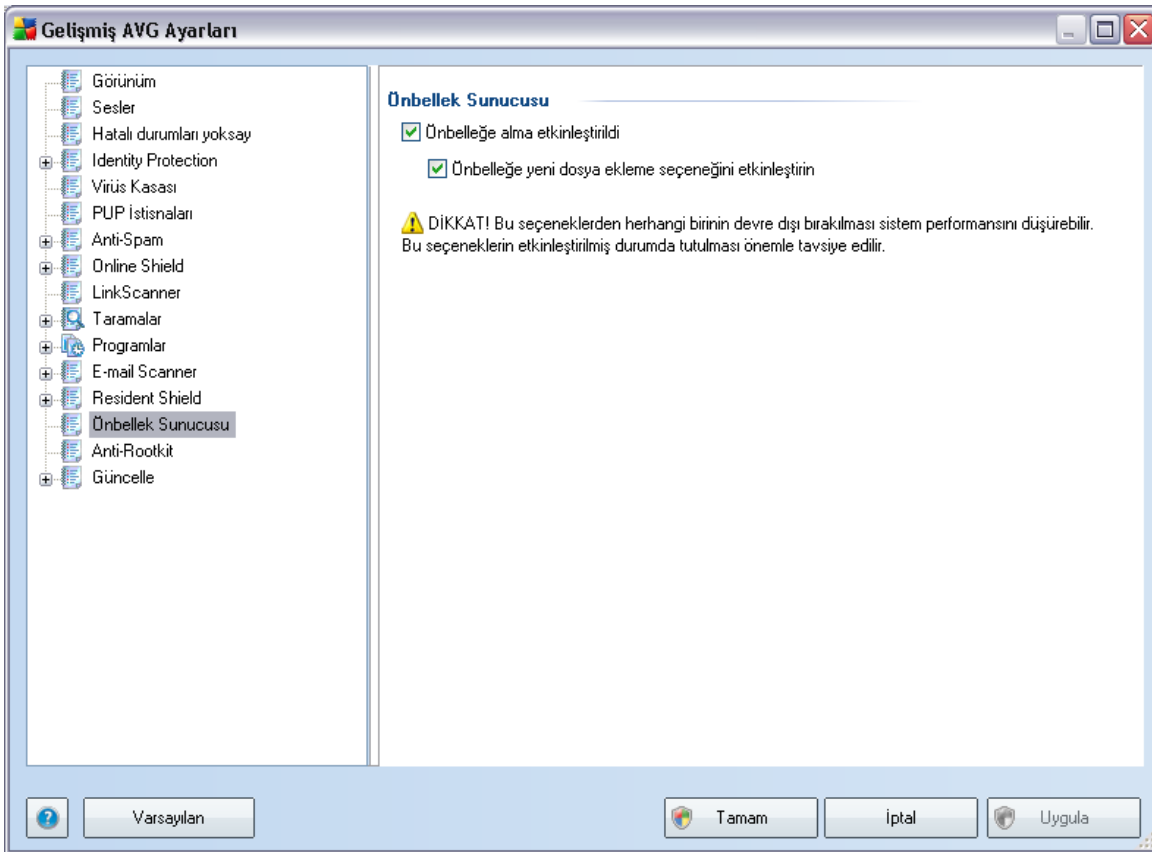
- **Ekle** – yerel diskin dolayım ağacından teker teker seçmek suretiyle tarama

isleminden hariç tutulacak dosyaları belirleyin.

- **Liste ekle**– [Yerlesik Kalkan](#) taramasından hariç tutulacak dosyalara ilişkin tam bir liste hazırlayabilmenizi sağlar
- **Düzenle** – seçilen dosyaya giden yolu düzenleyebilmenizi sağlar
- **Listeyi düzenle** – dosya listesini düzenlemenizi sağlar
- **Sil**– listeden seçilen dosyaya giden yolu silmenizi sağlar

10.12. Önbellek Sunucusu

Önbellek Sunucusu, herhangi bir taramayı hızlandırmak için tasarlanmış bir işlemidir (*istek üzerine tarama, programlanmış tüm bilgisayarı tarama, [Yerlesik Kalkan](#) taraması*). Güvenilir dosyaların bilgilerini toplar ve saklar (*dijital imzalı sistem dosyaları vb.*): Bu dosyalar, daha sonra güvenli olarak ele alınır ve tarama sırasında atlanır.

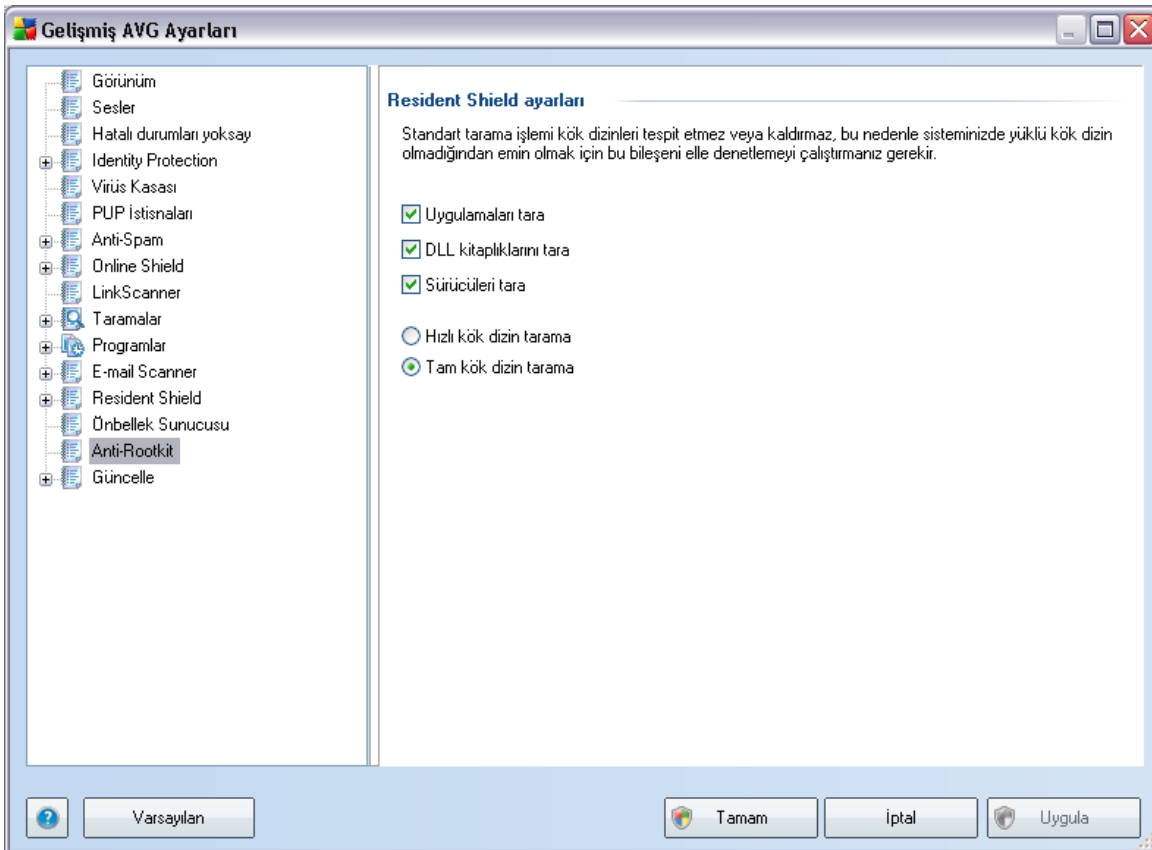


Ayarlar iletişim kutusu iki seçenek sunar:

- **Önbelleğe alma etkin** (varsayılan olarak açıktır) - **Önbellek Sunucusu**'nu kapatmak için kutunun isareti kaldırın ve önbellek belleğini boşaltın. Lütfen, kullandığınız her bir dosya virüs ve casus yazılım için ilk kez taranacağından taramanın yavaş olabileceğini ve bilgisayarınızın genel performansının azalacağını unutmayın.
- **Önbelleğe yeni dosyaların eklenmesini etkinleştir** (varsayılan olarak açıktır) - önbelleğe daha fazla dosya eklenmesini durdurmak için kutunun isaretini kaldırın. Önceden önbelleğe alınmış her dosya korunacak ve önbelleğe alma tamamen kapatılıncaya kadar veya virüs veritabanının bir sonraki güncellenmesine kadar kullanılacaktır.

10.13. Rootkit Önleme

Bu iletişim kutusunda **Anti-Rootkit** bileşenlerinin yapılandırmasını düzenleyebilirsiniz:





İletişim kutusu içinde sağlanan [Anti-Rootkit](#) bileşeninin tüm işlevlerinin düzenlenmesine **Anti-Rootkit bileşeninin arayüzünden** de ulaşabilirsiniz.

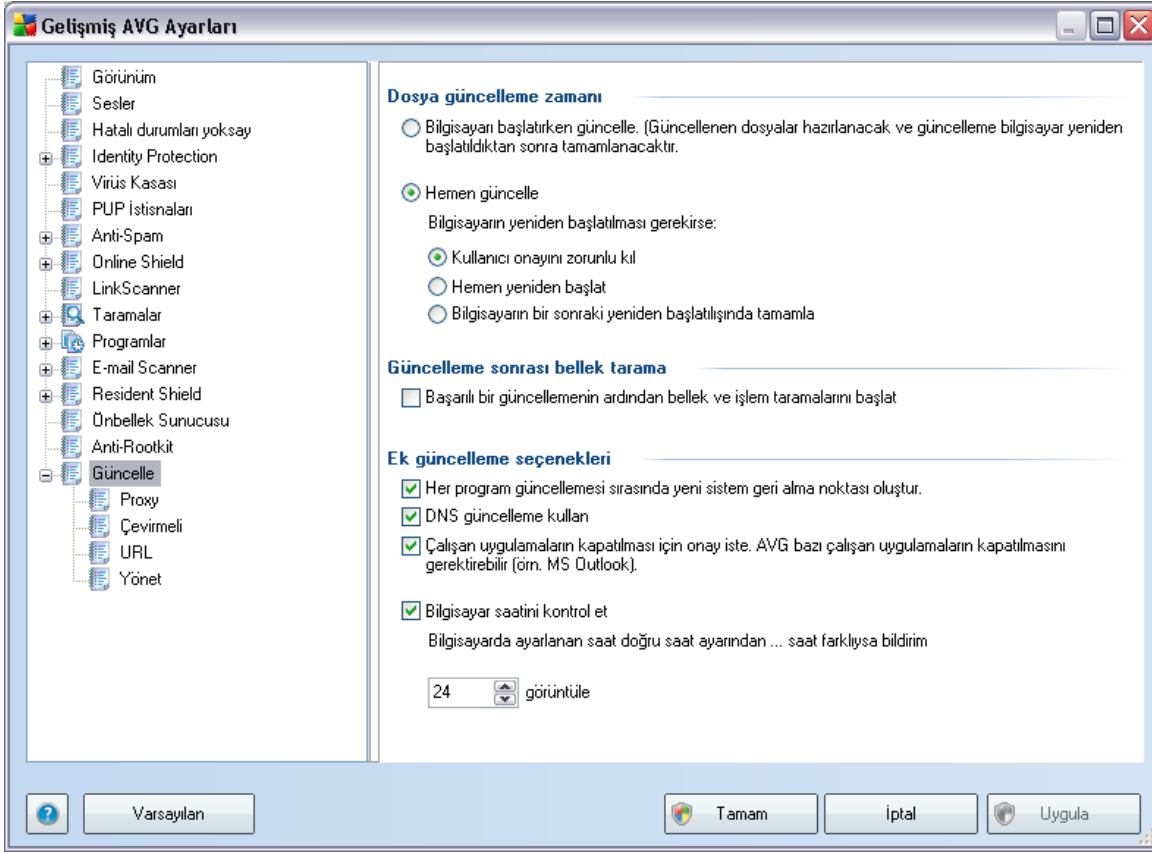
Taranmasını istediğiniz nesneleri belirlemek üzere ilgili kutuları işaretleyin:

- **Uygulamaları tara**
- **DLL kitaplıklarını tara**
- **Sürücülerini tara**

Bunun ardından kök kullanıcı tarama modunu da seçebilirsiniz:

- **Hızlı kök dizin tarama** - çalışan tüm işlemleri, yüklü sürücülerini ve sistem klasörlerini (genellikle *c:\Windows*) tarama
- **Tam kök dizin tarama** - çalışan tüm işlemleri, yüklü sürücülerini, sistem klasörünü (genellikle *c:\Windows*), ayrıca tüm yerel diskleri (*flash disk dahil, ancak disket/CD sürücülerini hariç*) tarama

10.14. Güncelle



Güncelleme navigasyonu ögesi, [AVG güncellemesine](#) ilişkin genel parametreleri belirleyebileceğiniz yeni bir iletişim kutusu açar:

Dosya güncelleme zamanı

Bu bölümde iki seçenek arasında seçim yapabilirsiniz: [güncelleme](#) bir sonraki bilgisayar açılışında yapılabilir ya da [güncellemeyi](#) hemen baslatabilirsiniz. Varsayılan olarak hemen güncelleme seçeneği seçilidir çünkü AVG bu şekilde maksimum güvenlik seviyesini temin edebilir. Güncellemenin bir sonraki bilgisayar açılışında gerçekleştirilmesi, ancak bilgisayarınızın günde en az bir kere açıldığından emin olduğunuz durumlarda önerilir.

Tüm varsayılan konfigürasyonu muhafaza etmek ve güncelleme işlemi hemen başlatmak istiyorsanız gerekli yeniden başlatma işleminin hangi şartlar altında

gerçekleştirileceğini belirleyebilirsiniz:

- **Kullanıcının onayını iste-** [işlemini tamamlamak üzere bilgisayarın yeniden başlatılacağını onaylamanız istenir](#)
- **Hemen yeniden başlat** - [güncelleme](#) işlemi tamamlanır tamamlanmaz onayınız istenmeden bilgisayarınız yeniden başlatılacaktır.
- **Bir sonraki bilgisayar başlangıcında tamamla** - [güncelleme işleminin](#) sonlandırılması bir sonraki bilgisayar açılışına ertelenecektir - aynı şekilde bu işlem, bilgisayarınızın günde en az bir kere açıldığından emin olduğunuz durumlarda önerilir.

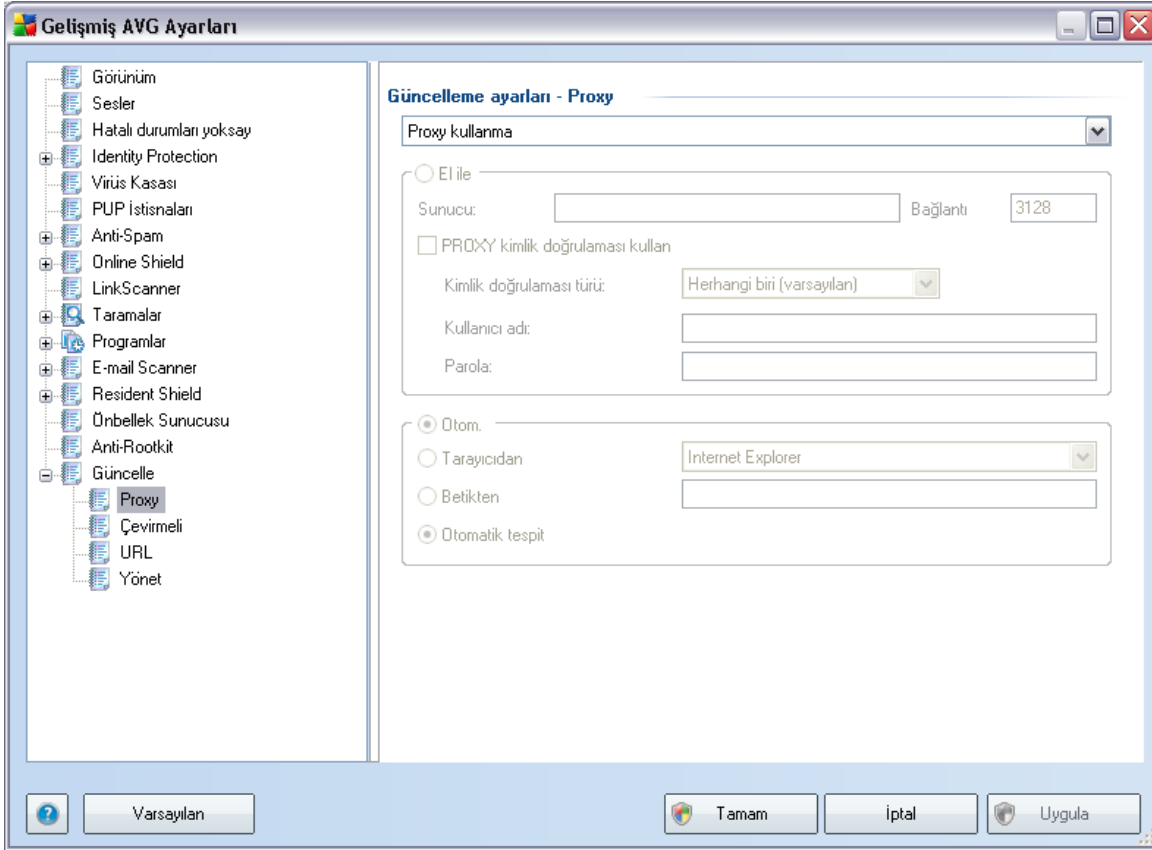
Güncelleme sonrası bellek tarama

Basarıyla tamamlanan her güncelleme sonrasında yeni bir bellek taraması başlatmak istediğinizi tanımlamak için bu onay kutusunu işaretleyin. En son indirilen güncelleme yeni virüs tanımlarını içerebilir ve bunlar taramaya hemen uygulanır.

Ek güncelleme seçenekleri

- **Her program güncellemesinden sonra sistem geri yükleme noktası olustur** - AVG programının güncelleme işlemi başlamadan önce geri yükleme noktası oluşturulur Güncelleme işleminin başarısız olması ve işletim sisteminizin çökmesi halinde işletme sisteminizi bu noktaya geri döndürebilirsiniz. Bu seçeneğe Baslat/Tüm Programlar bilgisayarınızın günde en az bir kere açıldığından emin olduğunuz durumlarda önerilir/Donatılar /Sistem Araçları / Sistem Geri Yükleme menüsünden erişebilirsiniz fakat değişikliklerin sadece uzman kullanıcılar tarafından yapılması önerilmektedir. Bu fonksiyonu kullanmak istiyorsanız bu kutucuğu işaretleyin.
- **DNS güncellemesini kullan** - güncelleme sunucusu ile AVG istemcisi arasında aktarılan veri miktarını minimize eden güncelleme dosyalarını tespit etme yöntemini kullanmak istediğinizi onaylamak için bu kutucuğu işaretleyin;
- **Çalışan uygulamaları kapatmak için onay iste** (varsayılan olarak açıktır) güncelleme işleminin tamamlanması için gerekirse izniniz olmaksızın geçerli olarak çalışan uygulamaların kapatılmamasını sağlayacaktır;
- **Bilgisayar saatini kontrol et** - bilgisayar saati ile doğru saat arasındaki fark belirlenen süreden uzun olduğunda bilgilendirilmek isterseniz bu seçeneği işaretleyin.

10.14.1. Proxy



Proxy sunucusu, Internet'e daha güvenli bir şekilde bağlanmanızı sağlayan bağımsız bir sunucu ya da bilgisayarınızda çalışan bir hizmet programıdır. Belirlenen ağ kuralları doğrultusunda, Internet'e doğrudan ya da bir proxy sunucusu üzerinden ulaşabilirsiniz; aynı anda her iki işleme de izin verilir. Bunun ardından **Güncelleme ayarları- Proxy** iletişim kutusunun ilk ögesinden aşağıdaki seçimleri yapmanız gerekmektedir:

- **Proxy kullan**
- **Proxy sunucusu kullanma** - varsayılan ayarlar
- **Proxy kullanarak bağlanmayı dene; başarısız olursa doğrudan bağlan**

Proxy sunucusunu kullanan herhangi bir seçeneği seçerseniz daha ayrıntılı bilgi girmeniz istenecektir. Sunucu ayarları manuel ya da otomatik olarak yapılandırılabilir.

Manüel yapılandırma

Manüel yapılandırmayı seçerseniz (ilgili iletişim kutusu bölümünü etkinleştirmek için **Manüel** seçeneğini işaretleyin) aşağıdaki bilgileri girmeniz gerekir:

- **Sunucu**– sunucunun IP adresini ya da sunucunun adını girin
- **Baglanti Noktası**– İnternet erişimine açık bağlantı noktasının numarasını girin (varsayılan olarak bu değer 3128 olarak atanmıştır fakat isteginiz doğrultusunda değiştirebilirsiniz – emin değilseniz lütfen ağ yöneticiniz ile irtibat kurun)

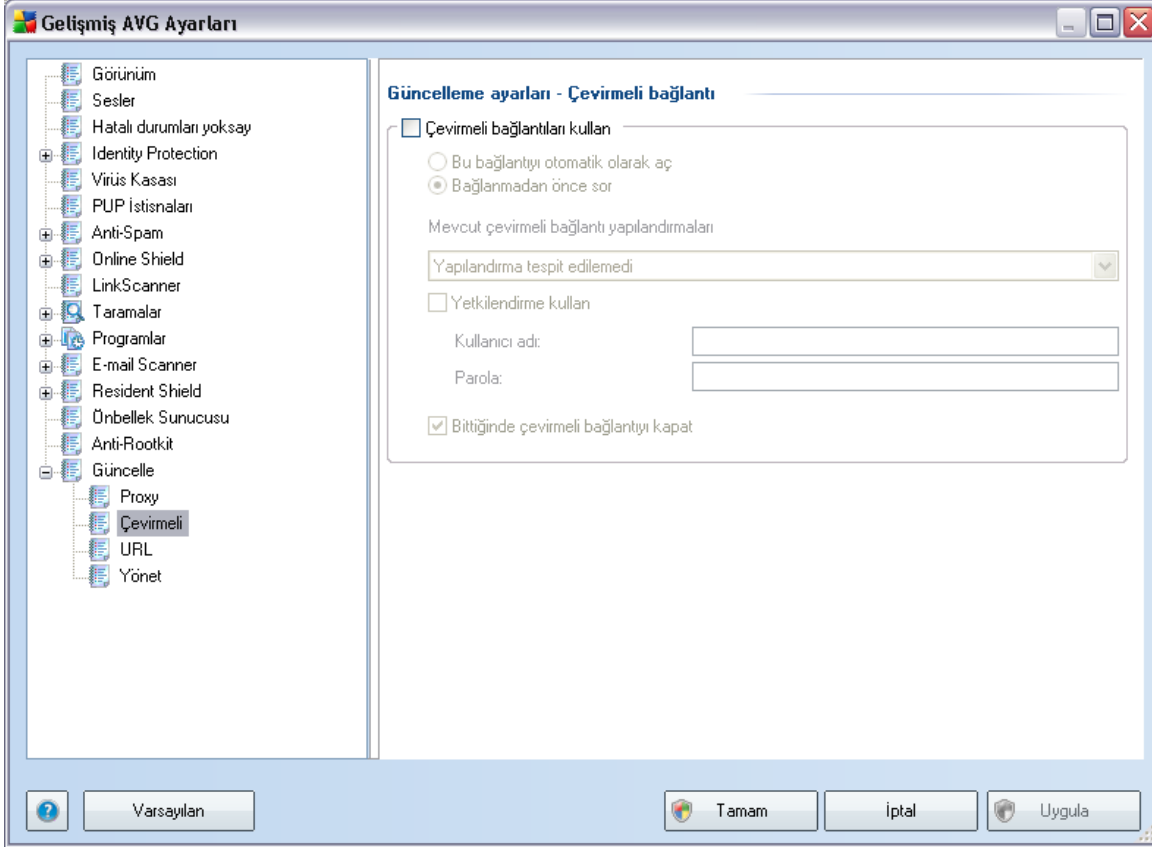
Proxy sunucusunda her kullanıcı için farklı kurallar yapılandırılabilir. Proxy sunucunuz bu şekilde yapılandırılmış ise proxy sunucusu üzerinden yapılan İnternet bağlantınıza ilişkin kullanıcı adı ve parolanızı onaylamak için **PROXY kimlik doğrulamasını kullan** seçeneğini işaretleyin.

Otomatik yapılandırma

Otomatik yapılandırmayı seçerseniz (ilgili iletişim kutusunu etkinleştirmek için **Oto** seçeneğini işaretleyin) ardından proxy yapılandırmasının nereden alınacağını belirleyin:

- **Tarayıcıdan** - Yapılandırma varsayılan İnternet tarayicinizden okunacaktır
- **Komut satırından** - yapılandırma, proxy adresine dönme fonksiyonu olan indirilmiş bir komut satırından okunacaktır
- **Otomatik Tespit Et** - yapılandırma otomatik olarak doğrudan proxy sunucusundan tespit edilecektir

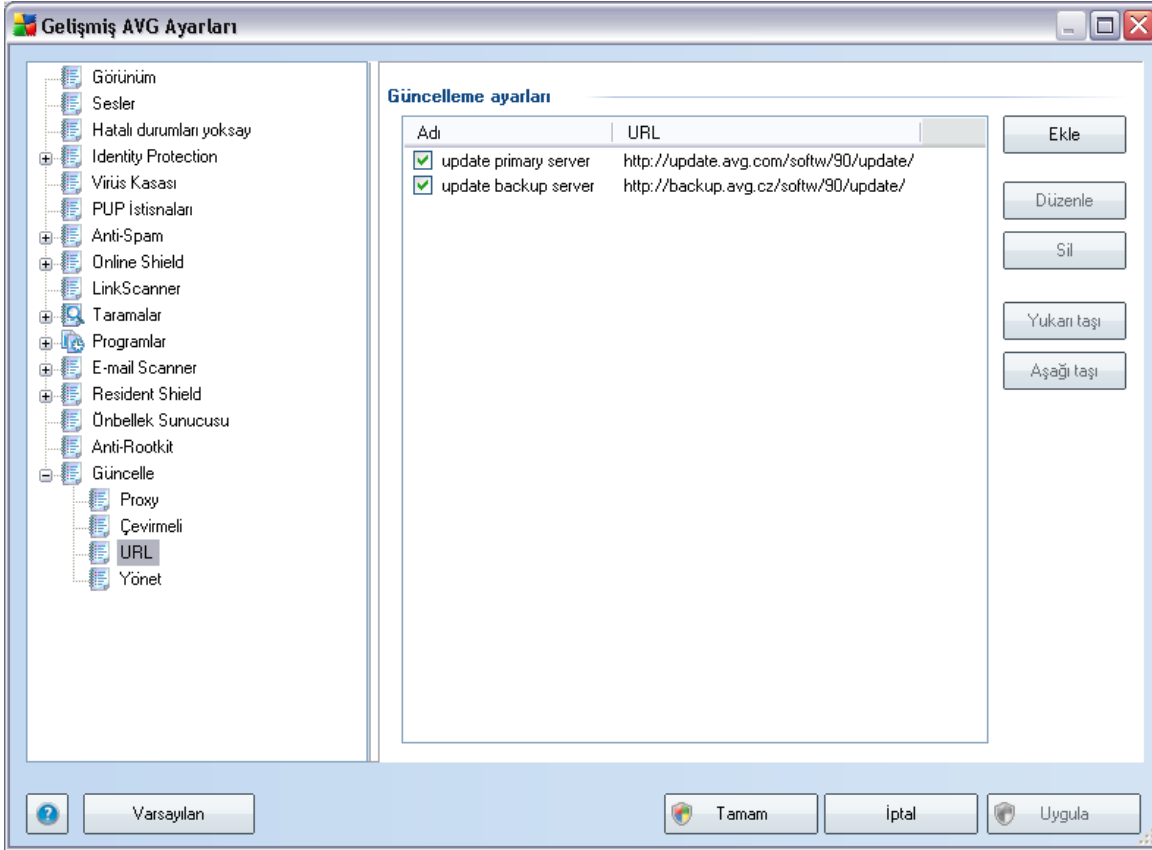
10.14.2. Çevirmeli



İsteğe bağlı olarak **Güncelleme ayarlarında tanımlanan tüm parametreler - Çevirmeli Bağlantı** iletişim kutusu Internet'e çevirmeli bağlantı ile bağlanılmasına iliskindir. **Çevirmeli bağlantı kullan** seçeneği seçilip alanlar etkinleştirilene kadar iletişim penceresinin alanları pasif olacaktır.

Internet'e otomatik olarak bağlanmak isteyip istemediğinizi (**Bu bağlantıyı otomatik olarak aç**) ya da bağlantıyı her seferinde manuel olarak kurmak isteyip istemediğinizi (**Bağlanmadan önce sor**) seçin. Otomatik bağlantılarda güncellemenin tamamlanmasının ardından bağlantının kesilmesini isteyip istemediğinizi de seçin (**Tamamlandığı zaman çevirmeli bağlantıyı kes**).

10.14.3. URL

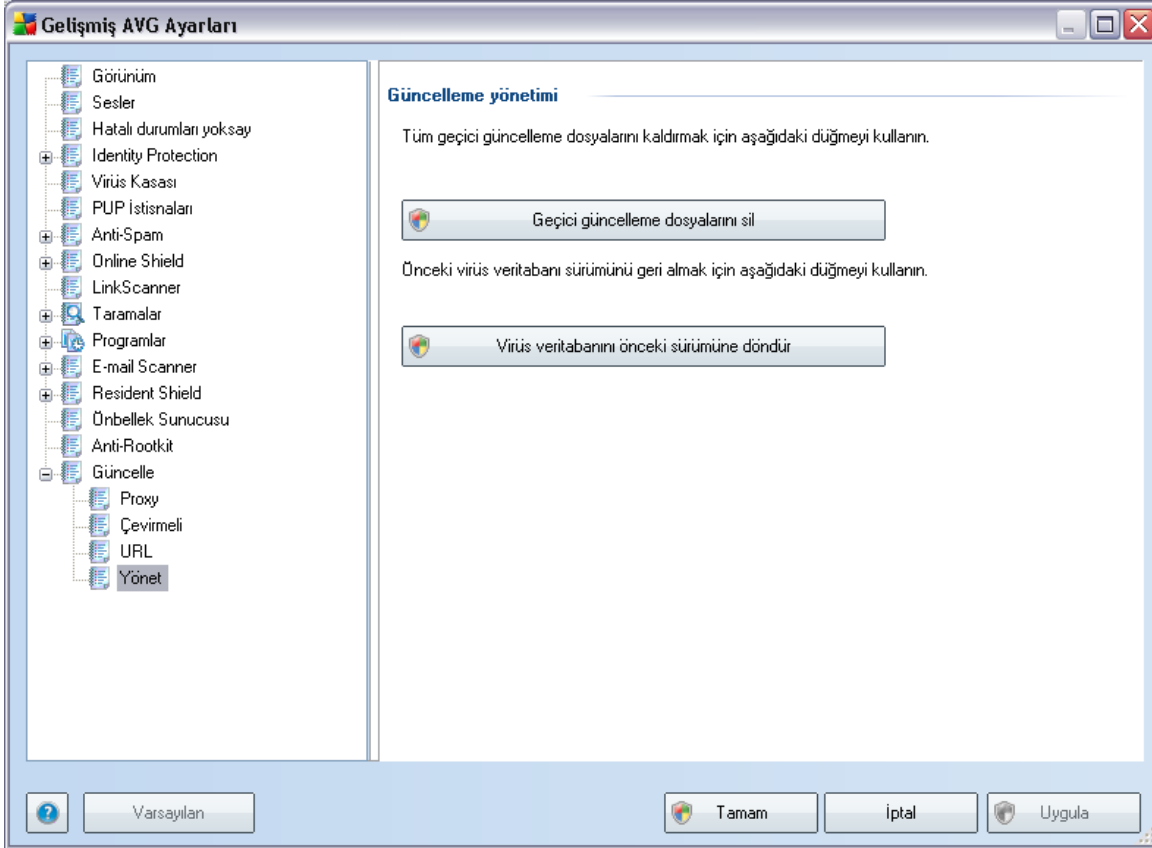


URL penceresinde güncelleme dosyalarının indirilebileceği bir dizi Internet adresi bulunur. Liste ve liste öğeleri aşağıdaki kontrol düğmeleri kullanılarak düzenlenebilir:

- **Ekle**– Listenize yeni bir URL eklemek için kullanacağınız pencereyi açar
- **Düzenle** - seçilen URL parametrelerini düzenleyebileceğiniz pencereyi açar
- **Sil**– seçilen URL'yi listeden seçer
- **Yukarı Tasi**– seçilen URL'yi listede bir sıra yukarı tasir
- **Asagi Tasi** - seçilen URL'yi listede bir sıra asagi tasir

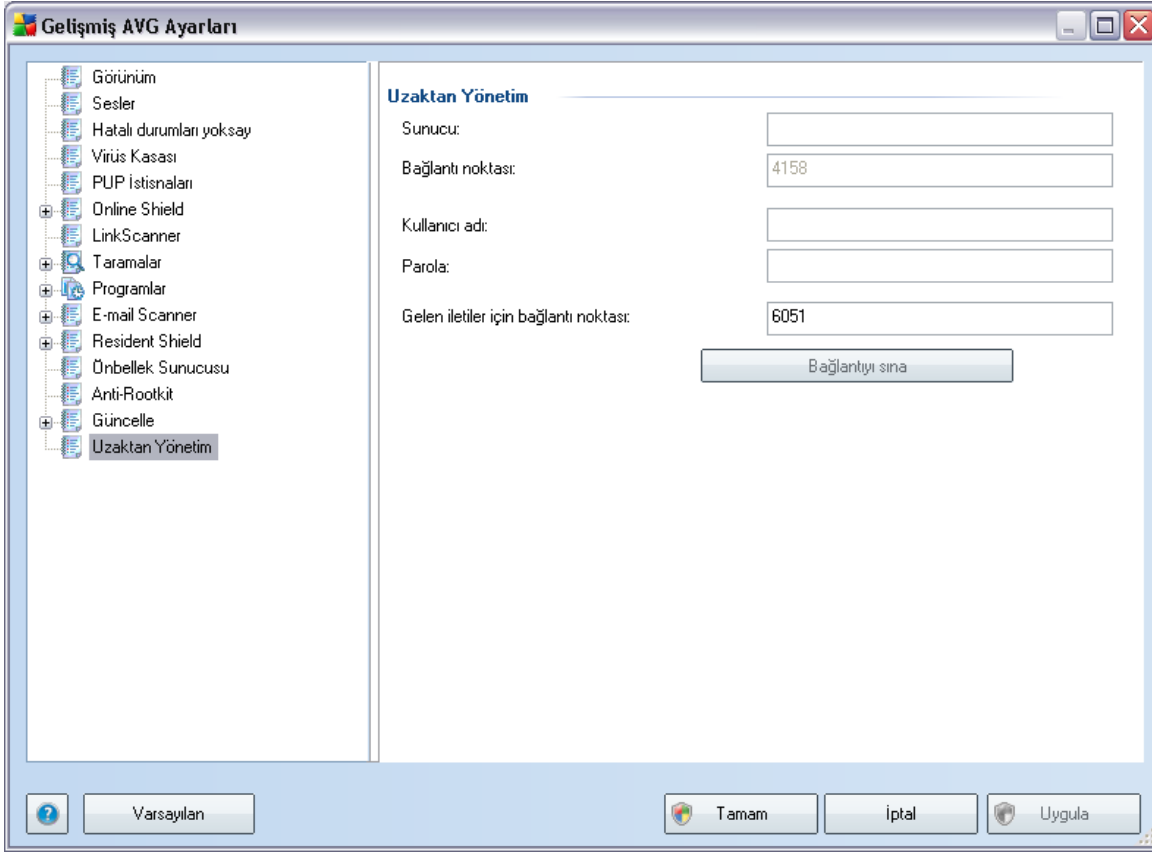
10.14.4. Yönet

Yönet iletişim penceresi, iki adet düğme ile ulaşılabilen iki seçenek sunmaktadır:



- **Geçici güncelleme dosyalarını sil** - tüm gereksiz güncelleme dosyalarını sabit diskinizden silmek için bu düğmeye basın (*öntanimli olarak söz konusu dosyalar 30 gün boyunca saklanır*)
- **Virüs veritabanını bir önceki sürüme döndür** – En güncel virüs veritabanını sabit diskinizden silmek ve daha önce kaydedilmiş sürüme dönmek için bu düğmeye basın (*yeni virüs tabanı sürümü, bir sonraki güncellemenin bir parçası olacaktır*)

10.15. Uzaktan Yönetim



Uzaktan Yönetim ayarları, AVG istemci istasyonunu uzak yönetici sisteme bağlamaya iliskindir. İlgili istasyonu uzaktan yönetime bağlamak istiyorsanız lütfen aşağıdaki parametreleri girin:

- **Sunucu** - AVG Admin Sunucusunun yüklü olduğu sunucu adı (ya da sunucunun IP adresi)
- **Bağlantı Noktası** - AVG istemcisinin AVG Admin Sunucusu ile iletişim kurdugu bağlantı noktası numarasıdır (*öntanımlı olarak 4158 numaralı bağlantı noktası kullanılmaktadır - bu bağlantı noktası numarasını kullanırsanız herhangi bir işlem yapmanıza gerek kalmaz*)
- **Oturum Açma Bilgileri** - iAVG istemcisi ile AVG Admin Sunucusu arasındaki ilişki güvenli bir bağlantı ise kullanıcı adınızı girin ...



- **Parola** - ... parolanizi girin
- **gelen mesajlar için bağlantı noktası** - AVG istemcisinin AVG Admin Suncusundan gelen mesajları kabul ettiği bağlantı noktası numarasıdır

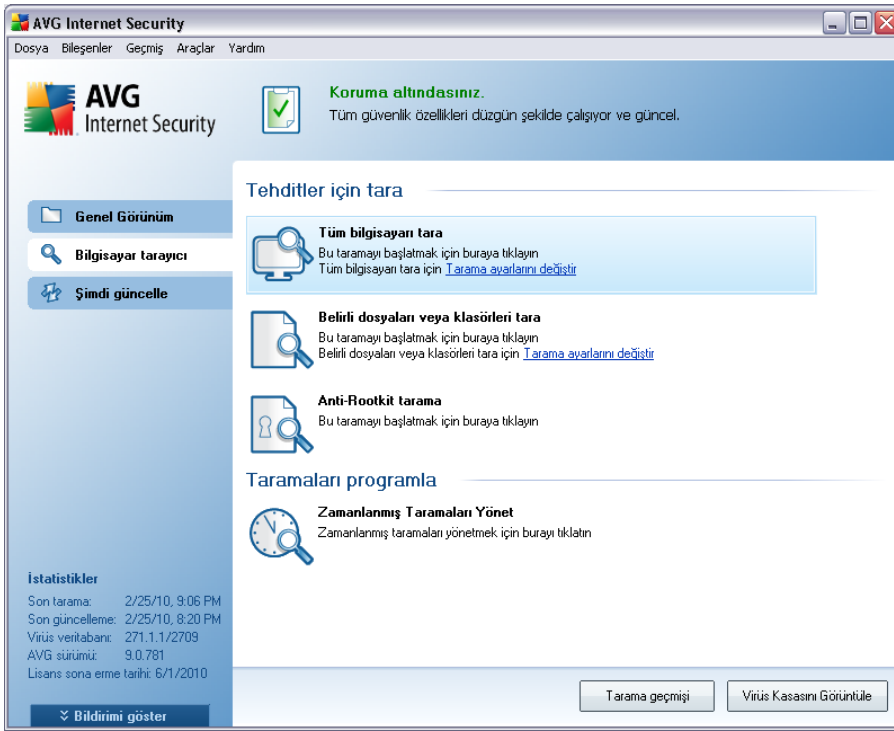
Baglantıyı sına düğmesi, yukarıda belirtilen verilerin tümünün geçerliliğini onaylamanıza yardımcı olur ve DataCenter'a başarıyla bağlanmak için kullanılabilir.

Not: Uzaktan yönetim konusunda ayrıntılı bilgi için lütfen AVG Network Edition dokümantasyonunu inceleyin.

11. AVG Tarama

Tarama, **AVG 9 Anti-Virus** islevinin önemli bir parçasıdır. Talebe uygun taramalar yapabilir ya da istediğiniz zamanlarda [periyodik taramalar planlayabilirsiniz](#).

11.1. Tarama Arayüzü



AVG tarama arayüzüne, ***Bilgisayar tarayıcısı*** [hızlı bağlantısından](#) ulaşabilirsiniz. ***Tehditleri tara*** iletişim kutusuna geçmek için bu bağlantıyı tıklayın. Bu iletişim kutusunda aşağıdakiler bulunmaktadır:

- [öntanimli taramalara](#) genel bakış - yazılım satıcısı tarafından tanımlanan üç tarama türü isteğe bağlı olarak hemen veya programlı olarak kullanılmaya hazırdir:
 - o [Tüm bilgisayarı tara](#)
 - o [Belirli dosyaları veya klasörleri tara](#)
 - o **Rootkit Önleme tarama**

- [tarama programlama](#) bölümü - İhtiyacınız doğrultusunda yeni programlar oluşturabilir ya da yeni taramalar tanımlayabilirsiniz.

Kontrol düğmeleri

Tarama arayüzünde bulunan genel kontrol düğmeleri şunlardır:

- **Tarama geçmişi** - tüm tarama geçmişi ile birlikte [Tarama sonuçlarına genel bakış](#) iletişim kutusunu açar
- **Virüs Kasesini Görüntüle** - tespit edilen bulasmaların karantina altına alındığı [Virüs Kasesini](#) yeni bir pencerede açar.

11.2. Öntanımlı Taramalar

AVG 9 Anti-Virus programının ana özelliklerinden biri istek üzerine taramadır. İsteğe bağlı taramalar, muhtemel bir virüs hakkında şüpheye düştüğünüz an bilgisayarınızın istediğiniz zamanda istediğiniz zaman yapabileceğiniz taramalardır. Kısacası, bilgisayarınızda virüs olduğunu düşünmeseniz bile söz konusu taramaların düzenli aralıklarla yapılması önerilmektedir.

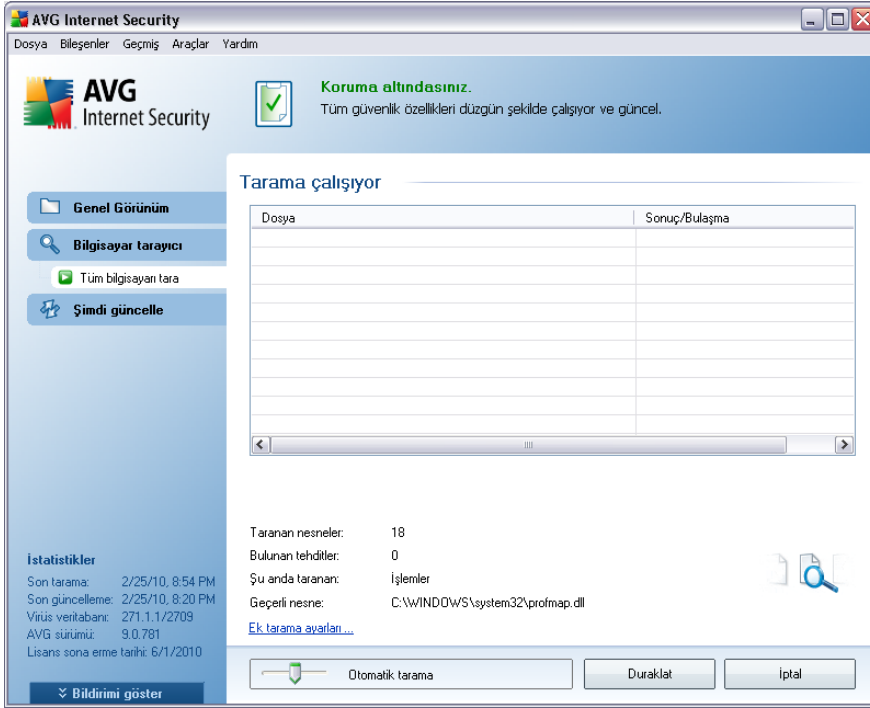
AVG 9 Anti-Virus içinde, yazılım satıcısının önceden tanımladığı iki tür tarama türü bulacaksınız:

11.2.1. Tüm Bilgisayarı Tara

Tüm bilgisayarı tara - tüm bilgisayarı muhtemel bulasmalara ve/veya potansiyel olarak istenmeyen programlara karşı tarar. Bu tarama, bilgisayarınızın tüm sabit disklerini tarayacak, virüsleri tespit edecek ve temizleyecek ya da tespit edilen bulasmayı [Virüs Kasesine](#) taşıyacaktır. Bilgisayarın tümühaftada en az bir defa taranmalıdır.

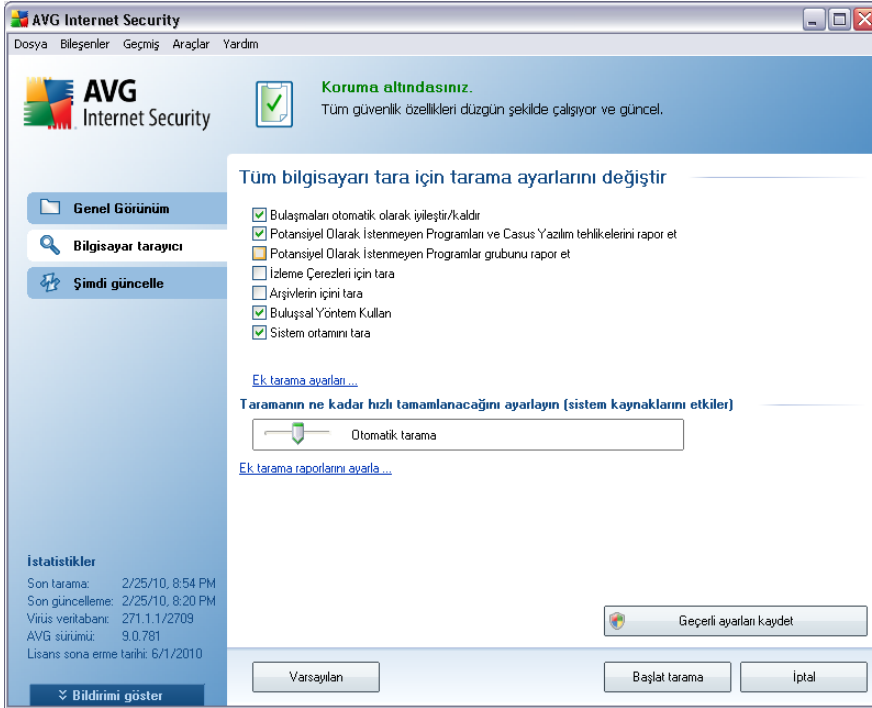
Tarama baslatma

Tüm bilgisayarı tara fonksiyonu tarama simgesine tıklamak suretiyle doğrudan [tarama arayüzünden](#) başlatılabilir. Bu tarama türü için baska belirli ayarlamaların yapılmasına gerek yoktur, tarama **Tarama yapıyor** iletişim kutusunda anında başlayacaktır(*bkz. ekran görüntüsü*). Tarama işlemi gerekirse geçici olarak kesilebilir (**Duraklat**) ya da iptal edilebilir (**Durdur**).

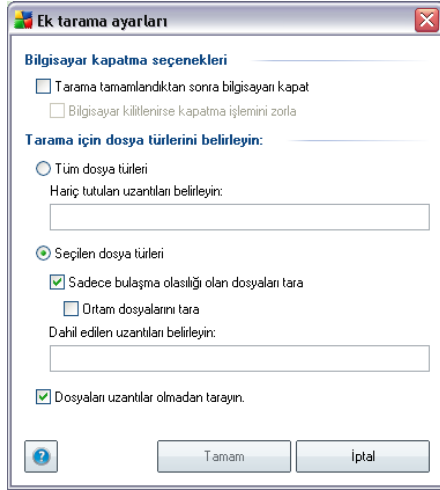


Tarama yapılandırması düzenleme

Tam bilgisayar taraması fonksiyonunun öntanımlı varsayılan ayarlarını düzenleme opsiyonunuz da bulunmaktadır. **Tarama ayarlarını değiştir** bağlantısına tıklayarak **Tüm bilgisayar taramasına ilişkin tarama ayarlarını değiştir** iletişim kutusuna gidin. **Varsayılan ayarları değiştirmeniz için geçerli bir nedeniniz olmadığı müddetçe bu ayarları korumanız önerilir!**

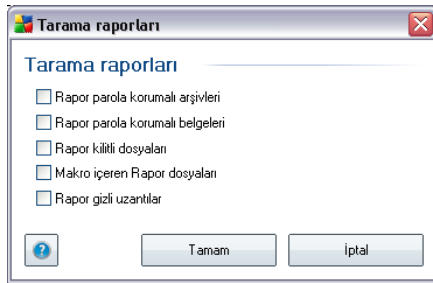


- **Tarama parametreleri** - tarama parametreleri listesindeki belirli parametreleri istediniz doğrultusunda açıp kapatabilirsiniz. Varsayılan olarak parametrelerin çoğu açıktır ve tarama sırasında otomatik olarak kullanılacaktır.
- **Ek tarama ayarları** - Bağlantı, bu parametreleri belirtebileceğiniz yeni bir **Ek tarama ayarları** iletişim kutusu açar:



- o **Bilgisayar kapatma seçenekleri** - Çalışan tarama işlemi bittiginde bilgisayarın otomatik olarak kapatılması gerekip gerekmediğine karar verir. Bu seçeneği seçerseniz (**Tarama bittikten sonra bilgisayarı kapat**) bilgisayar mevcut durumda kilitli olsa bile bilgisayarın kapatılmasını sağlayan bir seçeneğin bulunduğu bir pencere açılacaktır (**Bilgisayar kilitliyse bilgisayarı kapanmaya zorla**).
- o **Tarama için dosya türlerini tanımla** - Nelerin taranmasını istediğine de karar vermelisiniz:
 - **Tüm dosya türleri** taranmaması gereken virgülle ayrılmış dosya uzantılarının listesini sağlayarak taramada istisnaları tanımlama seçeneğiyle;
 - **Seçili dosya türleri** - Yalnızca virüs bulaşabilme olasılığı olan dosyaları taramayı istediğinizi belirtebilirsiniz (*virüs bulaşmayan dosyalar taranmayacaktır, örneğin, bazı düz metin dosyaları veya bazı diğer çalıştırılmayan dosyalar*); ortam dosyaları (*video, ses dosyaları - bu onay kutusunun işaretini kaldırırsanız, bu dosyalar genellikle çok büyük olduğundan ve virüs bulaşma olasılıkları çok az olduğundan tarama süresini daha da azaltır*). Tekrar, her zaman taranması gereken dosyaları uzantılarına göre belirtebilirsiniz.
 - İsteğe bağlı olarak, **Uzantıları olmayan dosyaları taramaya** da karar verebilirsiniz - bu seçenek varsayılan olarak açıktır ve gerçekten bir nedeniniz yoksa değiştirmemeniz önerilir. Uzantısı olmayan dosyalar süpheli olabilir ve her zaman taranmalıdır.

- **Tarama işlemi önceliği** - tarama işlemi önceliğini değiştirmek için kaydırma çubuğunu kullanabilirsiniz. Varsayılan olarak öncelik, sistem kaynaklarının kullanımını ve tarama işleminin hızını optimize eden orta seviyeye ayarlanmıştır (*Otomatik tarama*). Buna alternatif olarak, sistem kaynakları kullanımını minimize etmek için tarama işlemini daha yavaş (*bilgisayarda çalışmanız gerektiği ve taramanın ne kadar sürdüğünü önemsemediğiniz durumlar için uygundur*), ya da sistem kaynaklarını oldukça yoğun kullanmak suretiyle daha hızlı (*Örn. bilgisayar geçici olarak kimse kullanmayacak ise*) gerçekleştirebilirsiniz.
- **Tarama raporu oluşturma** - bağlantı üzerinden **Tarama Raporları** isimli bir iletişim kutusu açılır ve buradan ne tip buluntuların rapor edileceğini seçebilirsiniz:



Uyarı: Bu tarama parametreleri, yeni tanımlanan taramanın parametreleri ile aynıdır - [AVG Taraması / Tarama Planlama / Tarama Tipi](#) bölümünde açıklandığı doğrultuda. **Tüm bilgisayar tarama** fonksiyonunun varsayılan yapılandırmasını değiştirmeye karar vererseniz yeni ayarlarınızı, belirli dosya ya da klasörlerin taraması için kullanılacak varsayılan yapılandırma olarak atayabilirsiniz.

11.2.2. Belirli Dosyaları veya Klasörleri Tarama

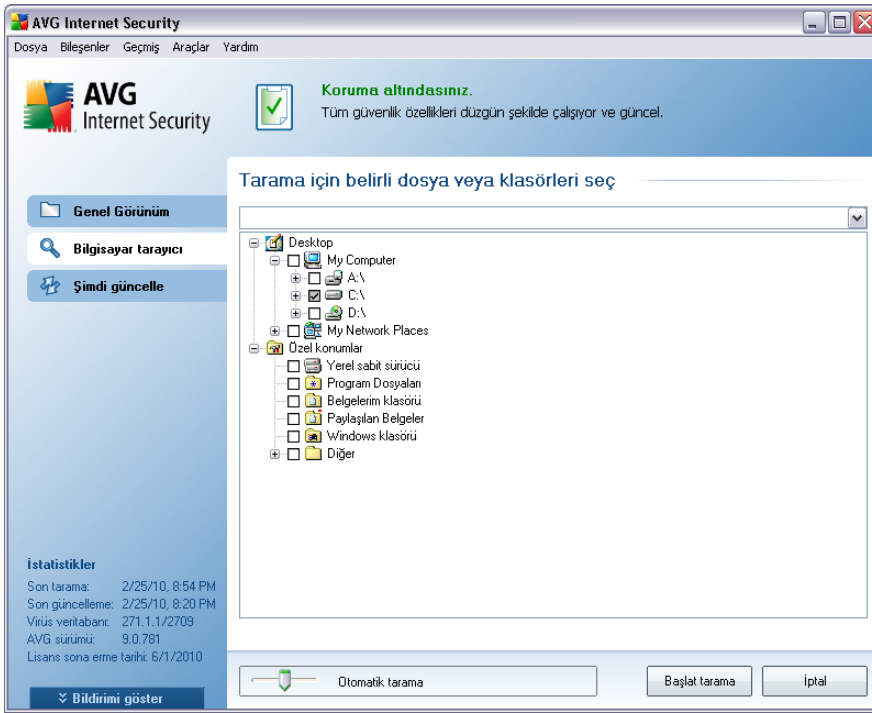
Belirli dosya ve klasörleri tarama - bilgisayarınızın sadece taraması için seçtiğiniz alanlarını tarama (*seçilen klasörler, sabit diskler, disket sürücüler, CD'ler vb.*). Virüs tespiti ve temizlenmesi sırasında tarama işlemi, tüm bilgisayar taraması ile aynıdır: bulunan virüsler temizlenir ya da [Virüs Kasesine](#) taşınır. Belirli dosya ve klasörlerin taraması, ihtiyaçlarınız doğrultusunda programladığınız taramalarda kullanılabilir.

Tarama başlatma

Belirli dosya ve klasörleri tarama fonksiyonu tarama simgesine tıklamak suretiyle doğrudan [tarama arayüzünden](#) başlatılabilir. Yeni bir **Tarama için belirli dosya ve klasörleri seçin** iletişim kutusu açılır. Bilgisayarınızın ağaç görünümünden taramasını istediğiniz klasörleri seçin. Seçilen klasörlerin her birine giden yol, otomatik olarak oluşturulacak ve iletişim kutusunun üst kısmındaki metin alanında görüntülenecektir.

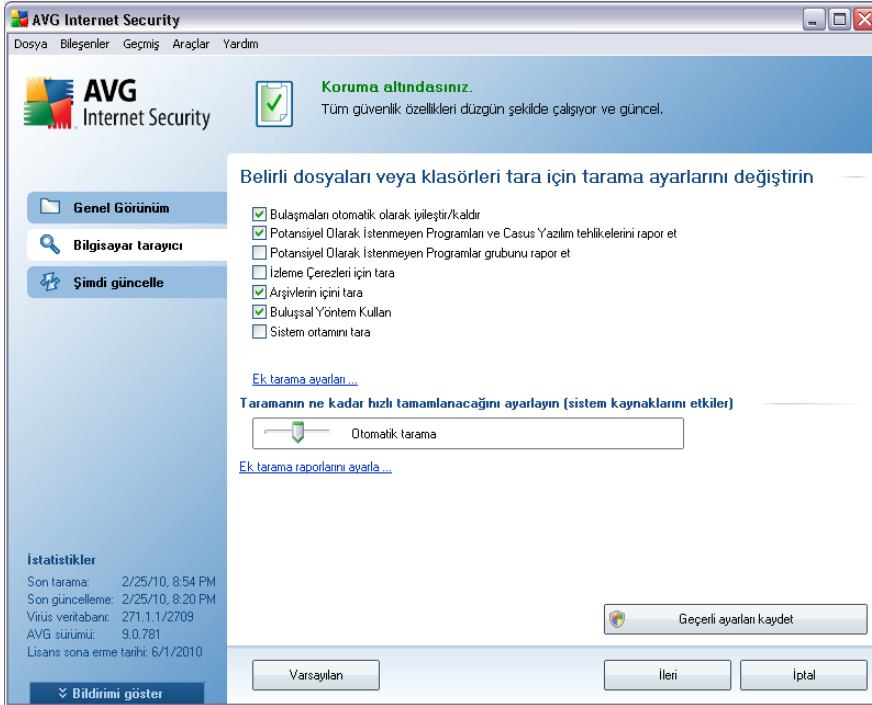
Belirli bir klasör taranırken içinde bulunan klasörlerin taranmaması gibi bir ihtimal de vardır; bunu yapabilmek için otomatik olarak oluşturulan yolun başına "-" işareti koyun (*ekran görüntülerini inceleyin*). Klasörün tümünü tarama dışında tutmak için "!" parametresini kullanın.

Son olarak taramayı başlatabilmek için **Taramayı başlat** düğmesine basın; tarama işleminin kendisi temel olarak [tam bilgisayar taraması](#) ile aynıdır.

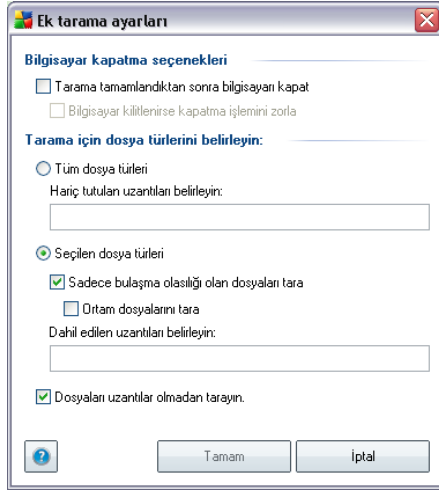


Tarama yapılandırması düzenleme

Belirli dosya ve klasörleri tara fonksiyonunun varsayılan ayarlarını düzenleme opsiyonunuz da bulunmaktadır. **Tarama ayarlarını değiştir** bağlantısına tıklayarak **Belirli dosya ve klasörlerin taranmasına ilişkin tarama ayarlarını değiştir** iletişim kutusuna gidin. **Varsayılan ayarları değiştirmeniz için geçerli bir nedeniniz olmadığı müddetçe bu ayarları korumanız önerilir!**

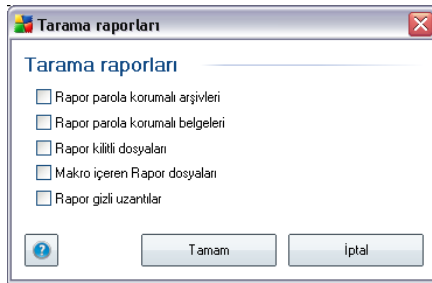


- **Tarama parametreleri** - tarama parametreleri listesindeki belirli parametreleri gerektiğinde açabilir ya da kapatabilirsiniz (*bu ayarlar hakkında ayrıntılı bilgi için lütfen [AVG Gelismis Ayarlar / Taramalar / Belirli Dosya veya Klasörleri Tara](#) bölümünü inceleyin*).
- **Ek tarama ayarları** - Bağlantı, su parametreleri belirtebileceğiniz yeni bir Ek tarama ayarları iletişim kutusu açar:



- o **Bilgisayar kapatma seçenekleri** - Çalışan tarama işlemi bittiginde bilgisayarın otomatik olarak kapatılması gerekip gerekmediğine karar verir. Bu seçeneği seçerseniz (**Tarama bittikten sonra bilgisayarı kapat**) bilgisayar mevcut durumda kilitli olsa bile bilgisayarın kapatılmasını sağlayan bir seçeneğin bulunduğu bir pencere açılacaktır (**Bilgisayar kilitliyse bilgisayarı kapanmaya zorla**).
- o **Tarama için dosya türlerini tanımla** - Nelerin taranmasını istediğinize de karar vermelisiniz:
 - **Tüm dosya türleri** taranmaması gereken virgülle ayrılmış dosya uzantılarının listesini sağlayarak taramada istisnaları tanımlama seçeneğiyle;
 - **Seçili dosya türleri** - Yalnızca virüs bulaşabilme olasılığı olan dosyaları taramayı istediğinizi belirtebilirsiniz (*virüs bulaşamayan dosyalar taranmayacaktır, örneğin, bazı düz metin dosyaları veya bazı diğer çalıştırılmayan dosyalar*); ortam dosyaları (*video, ses dosyaları - bu onay kutusunun işaretini kaldırırsanız, bu dosyalar genellikle çok büyük olduğundan ve virüs bulaşma olasılıkları çok az olduğundan tarama süresini daha da azaltır*). Tekrar, her zaman taranması gereken dosyaları uzantılarına göre belirtebilirsiniz.
 - İsteğe bağlı olarak, **Uzantıları olmayan dosyaları taramaya** da karar verebilirsiniz - bu seçenek varsayılan olarak açıktır ve gerçekten bir nedeniniz yoksa değiştirmemeniz önerilir. Uzantısı olmayan dosyalar şüpheli olabilir ve her zaman taranmalıdır.

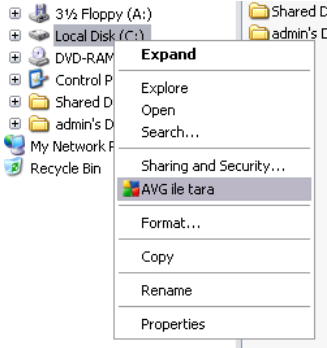
- **Tarama işlemi önceliği** - tarama işlemi önceliğini değiştirmek için kaydırma çubuğunu kullanabilirsiniz. Varsayılan olarak öncelik, sistem kaynaklarının kullanımını ve tarama işleminin hızını optimize eden orta seviyeye ayarlanmıştır (*Otomatik tarama*). Buna alternatif olarak, sistem kaynakları kullanımını minimize etmek için tarama işlemini daha yavaş (*bilgisayarda çalışmanız gerektiği ve taramanın ne kadar sürdüğünü önemsemediğiniz durumlar için uygundur*), ya da sistem kaynaklarını oldukça yoğun kullanmak suretiyle daha hızlı (*Örn. bilgisayar geçici olarak kimse kullanmayacak ise*) gerçekleştirebilirsiniz.
- **Tarama raporu oluşturma** - bağlantı üzerinden **Tarama Raporları** isimli bir iletişim kutusu açılır ve buradan ne tip buluntuların rapor edileceğini seçebilirsiniz:



Uyarı: Bu tarama parametreleri, yeni tanımlanan taramanın parametreleri ile aynıdır - [AVG Taraması / Tarama Planlama / Tarama Tipi](#) bölümünde açıklandığı doğrultuda. **Belirli dosya veya klasörleri tara** fonksiyonunun varsayılan yapılandırmasını değiştirmeye karar vererseniz yeni ayarlarınızı, belirli dosya ya da klasörlerin taraması için kullanılacak varsayılan yapılandırma olarak atayabilirsiniz. Buna ek olarak söz konusu yapılandırma tüm yeni programlanmış taramalarınız için sablon görevi görecek (tüm özelleştirilmiş taramalar, Seçilen dosya ya da klasörleri tara fonksiyonunun mevcut yapılandırmasına dayanmaktadır).

11.3. Windows Gezgini'nde Tarama

Bilgisayarın tümünde ya da seçilen bölümlerinde gerçekleştirilen öntanımlı taramaların yanı sıra **AVG 9 Anti-Virus**, doğrudan Windows Gezgini ortamında bulunan belirli nesnelerin hızlı bir şekilde taramasını da sağlamaktadır. Bilinmeyen bir dosyayı açmak istiyor fakat içeriginden emin olamıyorsanız isteğe bağlı olarak tarayabilirsiniz. Bu adımları takip edin:



- Windows Gezini'nde taramak istediginiz dosyayi (ya da klasörü) seçin
- Baglam menüsünü açmak için nesneye farenizle sag tiklatin
- **AVG ile Tara** seçenegini seçerek dosyanin AVG tarafından taranmasini saglayin

11.4. Komut Satırı Tarama

AVG 9 Anti-Virus içinde, taramayı komut satirindan çalıştırma seçeneği vardır. Söz konusu seçeneği, sunucularda ya da bilgisayar yeniden baslatıldıktan sonra otomatik olarak çalıştırılacak komut satirlarinin olusturulmasi sirasinda kullanabilirsiniz. Komut satirinda AVG'nin grafik kullanıcı arayüzünde sunulan parametrelerden daha fazlasini kullanarak tarama islemini gerçekleştirebilirsiniz.

AVG taramasını komut satirindan çalıştırmak için AVG'nin yüklendiği klasörde aşağıdaki komutu çalıştırın:

- **32 bit OS için avgscanx**
- **64 bit OS için avgscana**

Komut sözdizimi

Komut söz dizimi aşağıdaki gibidir:

- **Tam bilgisayar taramasi yapilirken avgscanx /parametre ...** Örn. **avgscanx /comp**
- **avgscanx /parametre /parametre ..** Birden fazla parametre kullanildigi zaman bunlar bir sıra halinde dizilmeli ve bir boslugun yani sıra bir de bölme isareti ile ayrilmalidir

- Parametrelerden biri için belirli bir deger verilmesi gerekiyorsa (**/scan** parametresi taranmak üzere bilgisayarınızın seçilen alanlari hakkında bilgi talep eder ve siz de seçilen kisma ilişkin veri yolunu tam olarak saglamaniz gerekir); degerler noktali virgöl ile birbirinden ayrilir, örn: **avgscanx /scan=C:\;D:**

Tarama parametreleri

Mevcut parametrelerin tam görünümümü görüntülemek için **/?** ya da **/HELP** (e.g. **avgscanx /?**). Zorunlu olan tek parametre, bilgisayarın hangi alanlarının taramasi gerektiğini belirlemek için kullanılan **/SCAN** parametresidir. Seçenekler hakkında daha ayrıntili açıklama almak için [komut satiri parametrelerine genel bakis](#) bölümüne bakın.

Tarama islemini baslatmak için **Enter** düğmesine basın. Tarama sırasında islemi **Ctrl+C** veya **Ctrl+Pause** tuslarına basarak durdurabilirsiniz.

Grafik arayüzünden çalıştırılan CMD taraması

Bilgisayarınızı Windows Güvenli Modda çalıştırdığınız zaman komut satiri taramasını grafik kullanıcı arayüzünden baslatma ihtimaliniz de bulunmaktadır. Taramanın kendisi komut satirından baslatılacaktır, **Komut Satiri Olusturucu** iletişim penceresi, en yaygın tarama parametrelerini konforlu grafik arayüzü vasıtasıyla görüntüler.

Söz konusu iletişim penceresine sadece Windows Güvenli Moddan ulaşılabilirdi için iletişim kutusu hakkında ayrıntili bilgi almak için doğrudan iletişim penceresinden açılan yardım dosyasını inceleyin.

11.4.1. CMD Tarama Parametreleri

Komut satiri taramasında kullanılan parametrelerin listesi aşağıda verilmiştir:

- **/SCAN** [Belirli dosya ya da klasörleri tara](#) /SCAN=path;path (e.g. /SCAN=C:\;D:\)
- **/COMP** [Bilgisayarı tamamen tara](#)
- **/HEUR** [Bulgusal analizi kullan](#)
- **/EXCLUDE** Tarama işleminden izin yolu veya dosyaları hariç tutun
- **/@** Komut dosyası /dosya adi/
- **/EXT** Bu uzantıları tarayın / örneğin EXT=EXE,DLL/

- **/NOEXT** u uzantilari tarama /örneğin NOEXT=JPG/
- **/ARC** Arsivleri tara
- **/CLEAN** Otomatik olarak temizle
- **/TRASH** Bulasan dosyalari [Virüs Kasasına taşı](#)
- **/QT** Hizli test
- **/MACROW** Makrolari rapor et
- **/PWDW** Parola ile korunan dosyalari rapor et
- **/IGNLOCKED** Kilitli dosyalari göz ardi et
- **/REPORT** /dosya adi/ dosyasina rapor et
- **/REPAPPEND** Rapor dosyasina ekle
- **/REPOK** Bulasmamis dosyalari Tamam olarak raporla
- **/NOBREAK** CTRL-BREAK ile islemin kesilmesine izin verme
- **/BOOT** MBR/BOOT kontrolünü etkinlestir
- **/PROC** Aktif islemleri tara
- **/PUP** [""Potansiyel olarak istenmeyen programlari""](#) rapor et
- **/REG** Kayit defterini tara
- **/COO** Çerezleri tara
- **/?** Bu konuyla ilgili yardimi görüntüle
- **/HELP** Bu konuyla ilgili yardimi görüntüle
- **/PRIORITY** Tarama önceligini belirle /Düşük, Oto, Yüksek/ (Bkz [Gelisimsi ayarlar / Taramalar](#))
- **/SHUTDOWN** Tarama tamamlandıktan sonra bilgisayari kapat
- **/FORCESHUTDOWN** Tarama tamamlandıktan sonra bilgisayari kapatmayi zorla

- /ADS

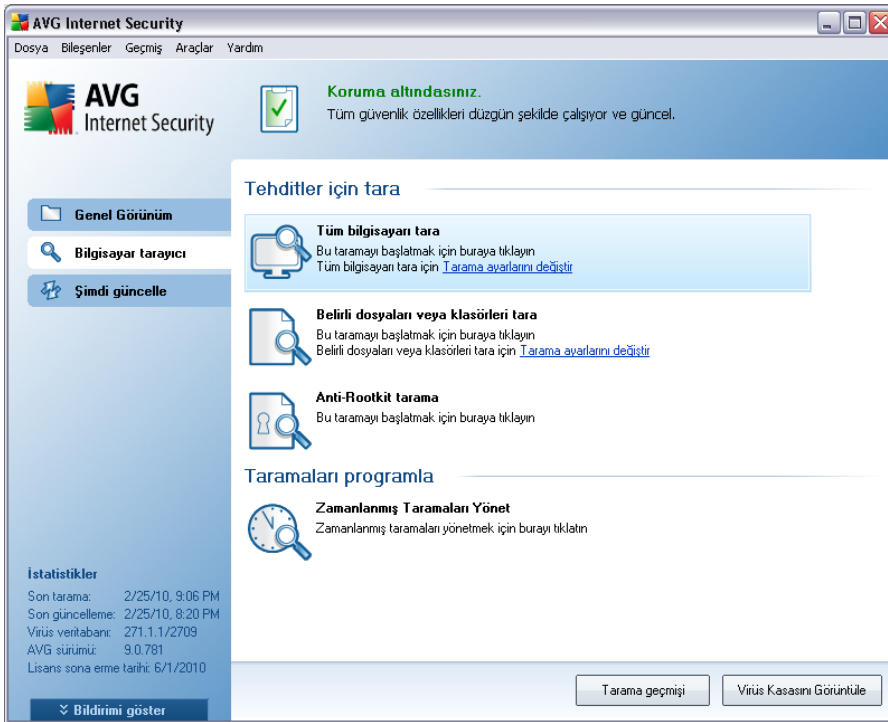
Alternatif Veri Akislarini Tara (sadece NTFS)

11.5. Tarama Planlama

AVG 9 Anti-Virus ile isteginiz dogrultusunda tarama yapmanin (örneğin bilgisayarınıza virüs bulastigindan süphelenirseniz) yani sıra programlanan bir plan dogrultusunda da tarama yapabilirsiniz. Taramaların bir program dogrultusunda yapılması önerilmektedir: bu şekilde, bilgisayarınızın virüs bulasma ihtimaline karşı korundugundan emin olursunuz ve ne zaman tarama yapmanız gerektiği konusunda endiselenmenize gerek kalmaz.

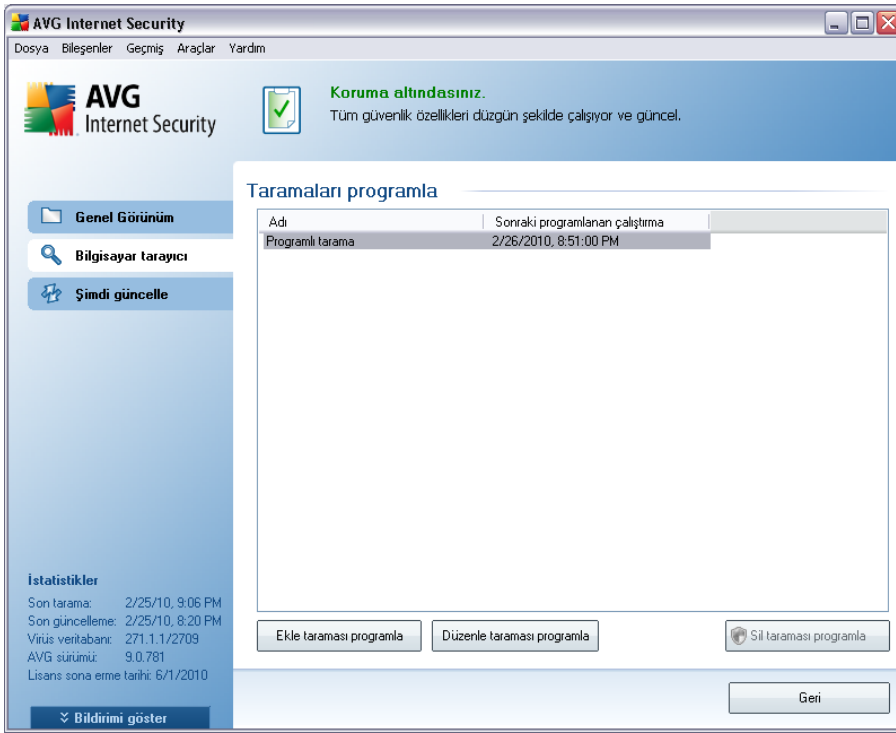
[Tüm bilgisayar taramasını](#) düzenli aralıklarla ve en azından haftada bir kere yapmanız gerekir. Diğer bir yandan, mümkün olması halinde programlı tarama yapılandırmasında ayarlandığı gibi tüm bilgisayar taramasını günlük olarak gerçekleştirin. Bilgisayarınız "daima açık" ise taramayı çalışma saatlerinden sonra gerçekleştirilecek şekilde programlayabilirsiniz. Bilgisayarınızı arada sırada kapatıyorsanız taramayı, taramaları [görev yerine getirilemediğinde bilgisayarın başlaması ile başlat](#) şeklinde programlayın.

Yeni tarama programları oluşturmak için [AVG tarama arayüzünü](#) inceleyin ve **Tarama programla** adi altındaki bölümü bulun:



Taramaları programla

Geçerli olarak zamanlanmış taramaların bir listesini bulabileceğiniz yeni bir **Taramaları programla** iletişim kutusunu açmak için **Taramaları programla** bölümündeki grafik simgeyi tıklatin:



Su kontrol düğmelerini kullanarak taramaları düzenleyebilir/ekleyebilirsiniz:

- **Tarama programı ekle** - düğme, **Programlanan tarama ayarları** iletişim kutusunu ve **Programlama Ayarları** sekmesini açar. Bu iletişim kutusunda yeni tanımladığınız taramanın parametrelerini belirleyebilirsiniz.
- **Tarama programını düzenle** - bu düğme, programlanan taramalar listesinden mevcut bir taramayı seçtiyseniz kullanılabilir. Bu durumda düğme etkinleşir ve **Programlanan tarama ayarları** iletişim kutusuna ve **Programlama ayarları** sekmesine geçmek için düğmeyi kullanabilirsiniz. Seçilen tarama parametreleri, zaten belirlenmiştir ve düzenlenebilir.
- **Tarama programını sil** - bu düğme, programlanan taramalar listesinden mevcut bir taramayı seçmeniz halinde etkinleşir. Bu tarama, ilgili kontrol

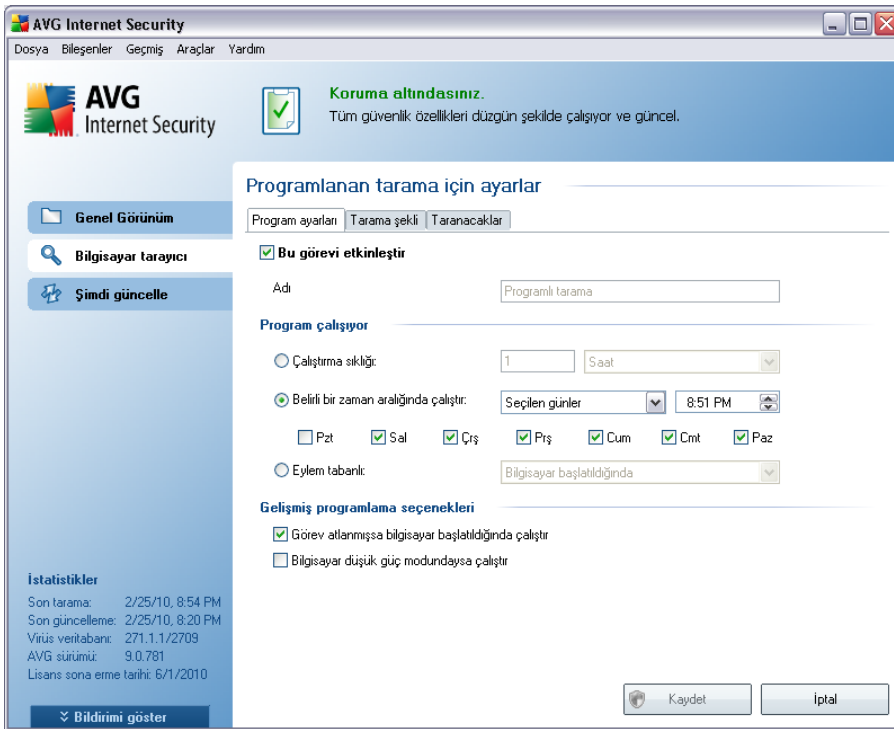


düğmesine basılarak listeden silinebilir. Diğer bir yandan sadece kendi taramalarınızı silebilirsiniz; **Tüm bilgisayar taraması programı** öntanımlıdır ve kesinlikle silinemez.

- **Geri** - [AVG tarama arayüzüne geri döner](#)

11.5.1. Program Ayarları

Yeni bir test programlamayı ve düzenli olarak başlamasını istiyorsanız, **Programlanan testin ayarları** iletişim kutusuna girin, (**Taramaları programla iletişim kutusundaki Tarama programı ekle** düğmesini tıklayın). Bu iletişim kutusu üç sekmeye ayrılmıştır: **Programlama ayarları** - aşağıdaki resme bakın (doğrudan yönlendirileceğiniz varsayılan sekmedir), **Tarama türü** ve **Taranacaklar**.



Planlama ayarları sekmesinde **Bu görevi etkinleştir** ögesini işaretleyerek ya da işareti kaldırarak planlanan taramayı geçici olarak devre dışı bırakabilir ve ihtiyaç duyduğunuzda yeniden açabilirsiniz.

Sonra oluşturmak ve programlamak üzere olduğunuz taramanın adını verin. **İsim** ögesini kullanarak metin alanına bir isim girin. Programladığınız taramaları diğerlerinden kolaylıkla ayırtabilmek için taramalarınıza kısa, açıklayıcı isimler vermeyi deneyin.

Örnek: Taramayı "Yeni Tarama" veya "Taramam" adıyla adlandırmanız uygun değildir çünkü bu adlar, taramanın fiilen neyi kontrol ettiğini açıklamaz. Diğer bir yandan "Sistem alanları taraması" oldukça açıklayıcı bir isim olacaktır. Ayrıca, taramanın adında söz konusu taramanın tam bilgisayar taraması ya da sadece seçilen dosya ya da klasörlerin taraması olup olmadığını belirtmenize gerek yoktur - taramalarınız [seçilen dosya ya da klasörleri tara](#) işlevinin farklı şekillerinden ibaret olacaktır.

Bu iletişim kutusunda taramanın aşağıdaki parametrelerini de tanımlayabilirsiniz:

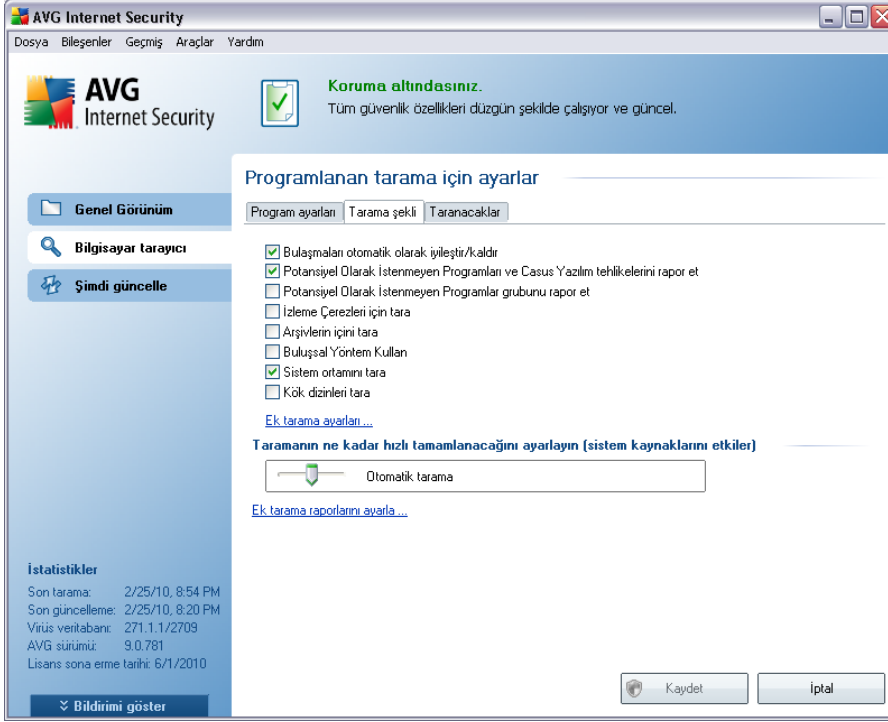
- **Planlama çalışıyor** - yeni planlanan taramanın başlaması için zaman aralığı girin. Zamanlama belirli bir sürenin ardından tekrarlanan tarama ile (**Her ...'de bir**) ya da kesin bir tarih ve saat tanımlayarak (**Belirli bir saatte çalıştır ...**), ya da (**Bilgisayar başlangıcında**) ilgili bir programın taramasıyla tanımlanabilir.
- **Gelişmiş planlama seçenekleri** - bu bölümde, bilgisayar düşük güç modundaydı veya tamamen kapatılmışsa hangi koşullar altında taramanın başlatılması/baslatılmaması gerektiğini belirleyebilirsiniz.

Programlı tarama iletişim kutusuna dair ayarların kontrol düğmeleri

Programlı tarama ayarları iletişim kutusunun üç sekmesinde (**Programlama ayarları**, [Tarama şekli](#) ve [Taranacaklar](#)) iki kontrol düğmesi bulunmaktadır ve hangi sekmede olduğunuz önemli olmaksızın aşağıdaki düğmelerin fonksiyonları aynıdır:

- **Kaydet** - bu sekmede veya bu iletişim kutusunun başka herhangi bir sekmesinde gerçekleştirdiğiniz tüm değişiklikleri kaydeder ve [AVG tarama arayüzü varsayılan penceresine](#) geri döner. Bu nedenle tüm sekmelerdeki test parametrelerini yapılandırmak istiyorsanız gereksinimlerinizin tamamını belirledikten sonra bunları kaydetmek için düğmeye basın.
- **İptal**- bu iletişim kutusunun bu sekmesinde veya başka bir sekmesinde yaptığınız değişiklikleri iptal eder ve [AVG tarama arayüzü varsayılan iletişim kutusuna](#)

11.5.2. Tarama Şekli



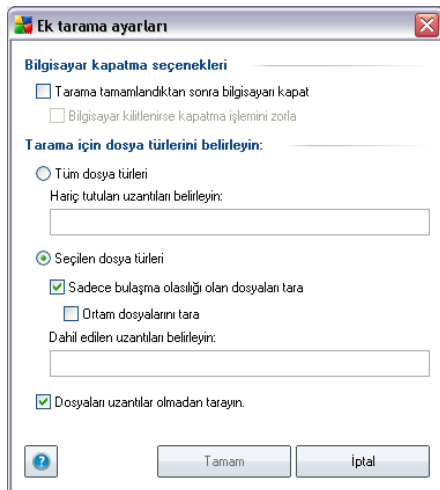
Tarama Sekli sekmesinde, isteğe bağlı olarak açılıp/kapatılabilen tarama parametrelerine ilişkin bir liste bulabilirsiniz. Varsayılan olarak birçok parametre devreye sokulur ve işlevsellik de tarama sırasında uygulanacaktır. Söz konusu ayarları değiştirmek açısından geçerli bir nedeniniz yoksa varsayılan yapılandırmayı olduğu gibi muhafaza etmeniz önerilir:

- **Bulaşmayı otomatik temizle/sil** - (varsayılan olarak açıktır): tarama işlemi sırasında bir virüs tanımlanırsa ve temizlenmesi mümkün ise otomatik olarak temizlenir. Etkilenen dosyanın otomatik olarak silinmiyor olması halinde ya da bu seçeneği kapatmayı seçerseniz bir virüs tespit edildiğinde bilgilendirileceksiniz ve tespit edilen bulaşma hakkında ne yapılacağına karar vermek zorunda kalacaksınız. Önerilen işlem, bulaşmış dosyayı [Virüs Kasasına](#) kaldırmaktır.
- **Potansiyel Olarak İstenmeyen Programları ve Casus Yazılım tehlikelerini rapor et** - (varsayılan olarak açıktır): [Anti-Spyware](#) motorunu etkinleştirmek ve virüslerle birlikte casus yazılımları da kontrol etmek için işaretleyin. [Casus yazılım](#), kötü amaçlı yazılım olabilecek kategorisini temsil eder: bir güvenlik riski oluştursa da bu programlardan bazıları bilerek yüklenebilir. Bilgisayarınızın güvenliğini artırdığından, bu özelliği etkin durumda tutmanızı öneriyoruz

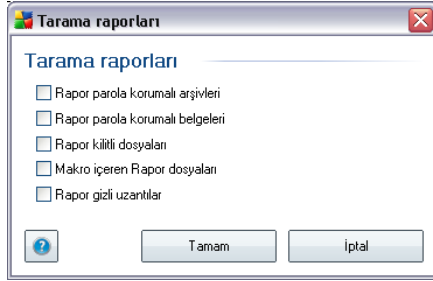
- **Gelismis Potansiyel Olarak Istemeyen Programlar setini bildir** - önceki seçenek etkinleştirilirse, genişletilmiş [casus yazılım](#) paketini algılamak için bu kutuyu da işaretleyebilirsiniz: doğrudan üreticiden alınan tamamen zararsız olan, ancak daha sonra kötüye kullanılan programlar. Bu, bilgisayar güvenliğinizi daha da artıran ek bir önlemdir, ancak yasal programları da engelleyebilir ve bu yüzden varsayılan olarak kapalıdır.
- **Tanımlama Bilgilerini Tara** - (varsayılan olarak açıktır): [Casus Yazılımdan Koruma](#) bileşeninin bu parametresi, tarama sırasında tespit edilmesi istenen tanımlama bilgilerini tanımlar (*HTTP tanımlama bilgileri site tercihleri ya da elektronik alışveriş sepeti içeriği gibi kullanıcı hakkında belirli bilgilerin toplanması, temin edilmesi ve izlenmesi için kullanılır*);
- **Arsivleri Tara** - (varsayılan olarak açıktır): Bu parametreler, tarama işleminin ZIP, RAR gibi belirli bir arşiv türü ile sıkıştırılmış olsa bile tüm dosyaları taramasını öngörür.
- **Bulgusal Analiz Kullan** - (varsayılan olarak açıktır): bulgusal analiz (*taranan nesnenin sanal bir bilgisayar ortamında dinamik olarak canlandırılması'na ilişkin talimatlar*) tarama sırasında kullanılacak virüs tespiti yöntemlerinden birisidir;
- **Sistem ortamını tara** - (varsayılan olarak açıktır): tarama işlemi, bilgisayarınızın sistem alanlarını da kontrol edecektir;

Sonra, tarama yapılandırmasını şu şekilde değiştirebilirsiniz:

- **Ek tarama ayarları** - Bağlantı, şu parametreleri belirtebileceğiniz yeni bir **Ek tarama ayarları** iletişim kutusu açar:



- o **Bilgisayar kapatma seçenekleri** - Çalışan tarama işlemi bittiginde bilgisayarın otomatik olarak kapatılması gerekip gerekmediğine karar verir. Bu seçeneği seçerseniz (**Tarama bittikten sonra bilgisayarı kapat**) bilgisayar mevcut durumda kilitli olsa bile bilgisayarın kapatılmasını sağlayan bir seçeneğin bulunduğu bir pencere açılacaktır (**Bilgisayar kilitliyse bilgisayarı kapanmaya zorla**).
- o **Tarama için dosya türlerini tanımla** - Nelerin taranmasını istediğine de karar vermelisiniz:
 - **Tüm dosya türleri** taranmaması gereken virgülle ayrılmış dosya uzantılarının listesini sağlayarak taramada istisnaları tanımlama seçeneğiyle;
 - **Seçili dosya türleri** - Yalnızca virüs bulaşabilme olasılığı olan dosyaları taramayı istediğinizi belirtebilirsiniz (*virüs bulaşmayan dosyalar taranmayacaktır, örneğin, bazı düz metin dosyaları veya bazı diğer çalıştırılmayan dosyalar*); ortam dosyaları (*video, ses dosyaları - bu onay kutusunun işaretini kaldırırsanız, bu dosyalar genellikle çok büyük olduğundan ve virüs bulaşma olasılıkları çok az olduğundan tarama süresini daha da azaltır*). Tekrar, her zaman taranması gereken dosyaları uzantılarına göre belirtebilirsiniz.
 - İsteğe bağlı olarak, **Uzantıları olmayan dosyaları taramaya** da karar verebilirsiniz - bu seçenek varsayılan olarak açıktır ve gerçekten bir nedeniniz yoksa değiştirmemeniz önerilir. Uzantısı olmayan dosyalar süpheli olabilir ve her zaman taranmalıdır.
- **Tarama işlemi önceliği** - tarama işlemi önceliğini değiştirmek için kaydırma çubuğunu kullanabilirsiniz. Varsayılan olarak öncelik, sistem kaynaklarının kullanımını ve tarama işleminin hızını optimize eden orta seviyeye ayarlanmıştır (*Otomatik tarama*). Buna alternatif olarak, sistem kaynakları kullanımını minimize etmek için tarama işlemini daha yavaş (*bilgisayarda çalışmanız gerektiği ve taramanın ne kadar sürdüğünü önemsemediğiniz durumlar için uygundur*), ya da sistem kaynaklarını oldukça yoğun kullanmak suretiyle daha hızlı (*Örn. bilgisayarı geçici olarak kimse kullanmayacak ise*) gerçekleştirebilirsiniz.
- **Tarama raporu oluşturma** - bağlantı üzerinden **Tarama Raporları** isimli bir iletişim kutusu açılır ve buradan ne tip buluntuların rapor edileceğini seçebilirsiniz:



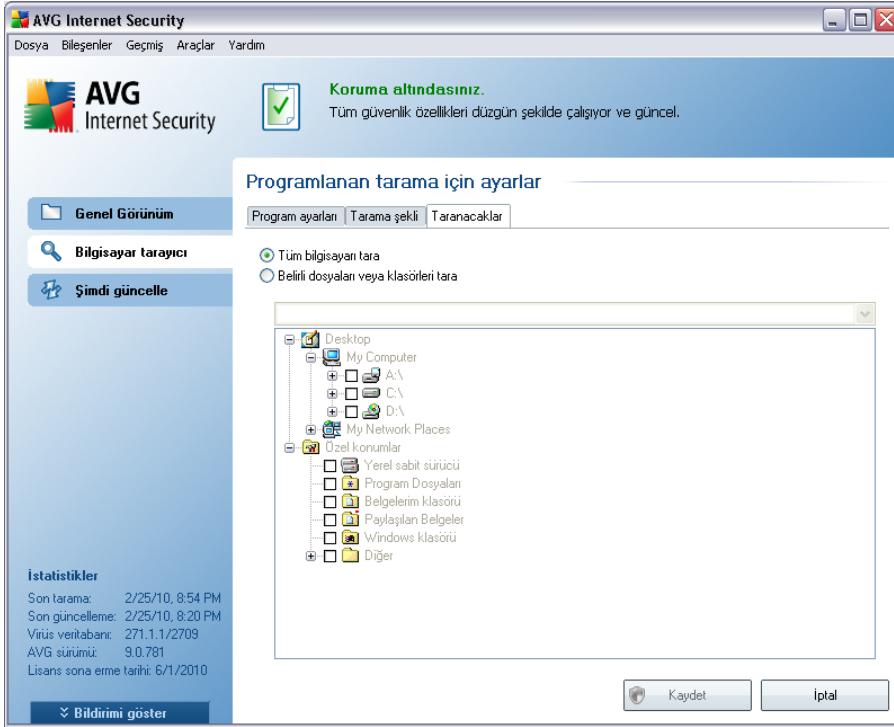
Not: Tarama yapılandırması varsayılan olarak optimum performansta gerçekleşecek şekilde ayarlanmıştır. Tarama ayarlarını değiştirmek için geçerli bir nedeniniz yoksa mevcut yapılandırmayı muhafaza etmeniz önerilmektedir. Yapılandırma, sadece deneyimli kullanıcılar tarafından değiştirilmelidir. Tarama yapılandırma hakkında daha fazla seçenek görmek için **Dosya / Gelismis ayarlar** sistem menüsünden ulaşabileceğiniz [Gelismis ayarlar](#) iletişim kutusunu açın.

Kontrol düğmeleri

Programlı tarama ayarları iletişim kutusunun her üç sekmesinde (**Programlama ayarları**, **Tarama şekli** ve **Taranacaklar**) iki kontrol düğmesi bulunmaktadır ve hangi sekmede olduğunuz önemli olmaksızın bunların fonksiyonları aynıdır:

- **Kaydet** - bu sekmede veya bu iletişim kutusunun başka herhangi bir sekmesinde gerçekleştirdiğiniz tüm değişiklikleri kaydeder ve [AVG tarama arayüzü varsayılan penceresine](#) geri döner. Bu nedenle tüm sekmelerdeki test parametrelerini yapılandırmak istiyorsanız gereksinimlerinizin tamamını belirledikten sonra bunları kaydetmek için düğmeye basın.
- **İptal**- bu iletişim kutusunun bu sekmesinde veya başka bir sekmesinde yaptığınız değişiklikleri iptal eder ve [AVG tarama arayüzü varsayılan iletişim kutusuna](#)

11.5.3. Taranacaklar



Taranacaklar sekmesinde, [tüm bilgisayarı tarama](#) veya [belirli dosya veya klasörleri taramayı](#) programlamak isteyip istemediğinizi belirleyebilirsiniz.

Belirli dosya ve klasörlerin taranmasını seçmeniz durumunda, bu iletişim kutusunun alt tarafında görüntülenen ağaç yapısı etkinleşir ve taranacak klasörleri belirleyebilirsiniz (*taramak istediğiniz klasörü buluncaya kadar artı isaretini tıklatarak öğeleri genişletin*). İlgili kutuları işaretleyerek birden fazla klasör seçebilirsiniz. Seçilen klasörler, iletişim kutusunun üstünde bulunan metin alanında görüntülenir; açılır menü seçilen tarama geçmişini daha sonra kullanılmak üzere saklar. Alternatif olarak, istediğiniz klasörün tam yolunu elle girebilirsiniz (*birden fazla yol girerseniz, bunları ekstra boşluk bırakmadan noktalı virgülle ayırmanız gerekir*).

Ağaç yapısı içinde **Özel konumlar** adında bir dal da görürsünüz. Aşağıda, ilgili onay kutusu işaretlendiğinde taranacak konumların listesi bulunmaktadır:

- **Yerel sabit sürücüler** - bilgisayarınızdaki tüm sabit sürücüler
- **Program dosyaları** - C:\Program Files\



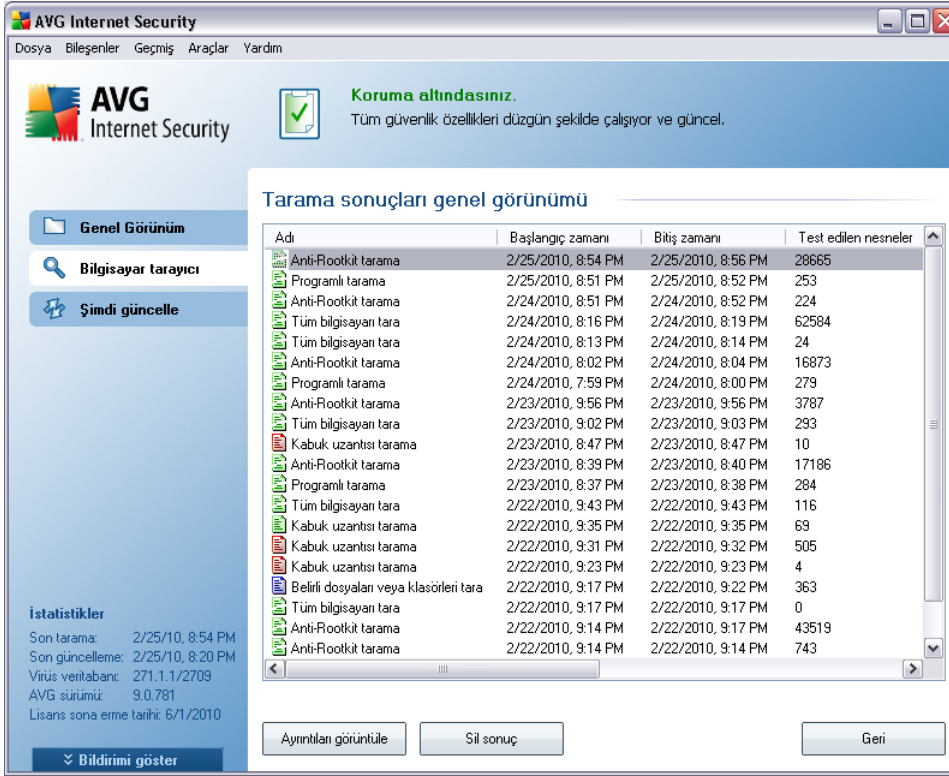
- **Belgelerim klasörü** - C:\Documents and Settings\Kullanici\Belgelerim\
- **Paylasilan Belgeler** - C:\Documents and Settings\All Users\Belgeler\
- **Windows klasörü** - C:\Windows\
- **Diger**
 - o *Sistem sürücüsü* - işletim sisteminin yüklü olduğu sabit sürücü (genellikle C:)
 - o *Sistem klasörü* - Windows/System32
 - o *Geçici Dosyalar klasörü* - Documents and Settings/Kullanici/Local Settings/Temp
 - o *Geçici İnternet Dosyaları* - Documents and Settings/Kullanici/Local Settings/Temporary Internet Files

Programli tarama iletisim kutusuna dair ayarlarin kontrol düğmeleri

Programli tarama ayarlari iletisim kutusunun üç sekmesinde (**Programlama ayarlari**, **Tarama sekli** ve **Taranacaklar**) iki kontrol düğmesi bulunmaktadır ve hangi sekmede olduğunuz önemli olmaksizin aşağıdaki düğmelerin fonksiyonları aynıdır:

- **Kaydet** - bu sekmede veya bu iletisim kutusunun baska herhangi bir sekmesinde gerçekleştirdiginiz tüm değişiklikleri kaydeder ve [AVG tarama arayüzü varsayılan penceresine](#) geri döner. Bu nedenle tüm sekmelerdeki test parametrelerini yapılandırmak istiyorsanız gereksinimlerinizin tamamını belirledikten sonra bunları kaydetmek için düğmeye basın.
- **İptal**- bu iletisim kutusunun bu sekmesinde veya baska bir sekmesinde yaptığınız değişiklikleri iptal eder ve [AVG tarama arayüzü varsayılan iletisim kutusuna geri döner](#).

11.6. Tarama Sonuçları Genel Görünümü



The screenshot shows the AVG Internet Security interface. The main window is titled "Tarama sonuçları genel görünümü". It features a table with columns: "Adı", "Başlangıç zamanı", "Bitiş zamanı", and "Test edilen nesneler". The table lists various scan results, including "Anti-Rootkit tarama", "Programlı tarama", "Tüm bilgisayar tarama", "Kabuk uzantısı tarama", and "Belirli dosyaları veya klasörleri tarama". Each row shows the scan name, start and end times, and the number of objects tested. On the left side, there are buttons for "Genel Görünüm", "Bilgisayar taramacı", and "Şimdi güncelle". Below these, there is a section for "İstatistikler" showing the last scan date, update date, virus definition version, AVG version, and license expiration date. At the bottom, there are buttons for "Ayrıntıları görüntüle", "Sil sonuç", and "Geri".

Adı	Başlangıç zamanı	Bitiş zamanı	Test edilen nesneler
Anti-Rootkit tarama	2/25/2010, 8:54 PM	2/25/2010, 8:56 PM	28665
Programlı tarama	2/25/2010, 8:51 PM	2/25/2010, 8:52 PM	253
Anti-Rootkit tarama	2/24/2010, 8:51 PM	2/24/2010, 8:52 PM	224
Tüm bilgisayar tarama	2/24/2010, 8:16 PM	2/24/2010, 8:19 PM	62584
Tüm bilgisayar tarama	2/24/2010, 8:13 PM	2/24/2010, 8:14 PM	24
Anti-Rootkit tarama	2/24/2010, 8:02 PM	2/24/2010, 8:04 PM	16873
Programlı tarama	2/24/2010, 7:59 PM	2/24/2010, 8:00 PM	279
Anti-Rootkit tarama	2/23/2010, 9:56 PM	2/23/2010, 9:56 PM	3787
Tüm bilgisayar tarama	2/23/2010, 9:02 PM	2/23/2010, 9:03 PM	293
Kabuk uzantısı tarama	2/23/2010, 8:47 PM	2/23/2010, 8:47 PM	10
Anti-Rootkit tarama	2/23/2010, 8:39 PM	2/23/2010, 8:40 PM	17186
Programlı tarama	2/23/2010, 8:37 PM	2/23/2010, 8:38 PM	284
Tüm bilgisayar tarama	2/22/2010, 9:43 PM	2/22/2010, 9:43 PM	116
Kabuk uzantısı tarama	2/22/2010, 9:35 PM	2/22/2010, 9:35 PM	69
Kabuk uzantısı tarama	2/22/2010, 9:31 PM	2/22/2010, 9:32 PM	505
Kabuk uzantısı tarama	2/22/2010, 9:23 PM	2/22/2010, 9:23 PM	4
Belirli dosyaları veya klasörleri tarama	2/22/2010, 9:17 PM	2/22/2010, 9:22 PM	363
Tüm bilgisayar tarama	2/22/2010, 9:17 PM	2/22/2010, 9:17 PM	0
Anti-Rootkit tarama	2/22/2010, 9:14 PM	2/22/2010, 9:17 PM	43519
Anti-Rootkit tarama	2/22/2010, 9:14 PM	2/22/2010, 9:14 PM	743

Tarama sonuçlarına genel bakış penceresine, [AVG tarama arayüzünde Tarama geçmişi](#) düğmesine basarak ulaşabilirsiniz. İletişim kutusunda, daha önce baslatılan tüm taramalar ve sonuçları hakkında bilgi bulunmaktadır.

- **Adı** - taramanın amacı; [öztanımlı taramalardan](#) birinin adı ya da [programladığınız taramaya](#) verdığınız adlardan biri olabilir. Her ismin yanında tarama sonucunu belirten bir simge bulunmaktadır:

 - yeşil simge tarama sırasında herhangi bir bulaşmanın tespit edilemediğini gösterir

 - mavi simge tarama sırasında bir bulaşmanın tespit edildiğini ancak bulaşmış nesnenin otomatik olarak silindiğini gösterir

 - kırmızı simge tarama sırasında bir bulaşmanın tespit edildiğini, ancak bulaşmış nesnenin silinemediğini gösterir!

Simgeler bütün halinde ya da yarisi kesilmiş olabilir - bütün halindeki simge, tarama isleminin dogru sekilde tamamlandigini ve bitirildigini gösterirken yarisi kesilmiş simge, taramanın iptal edildigini ya da kesildigini gösterir.

Not: Taramaların her biri hakkında ayrıntılı bilgi almak için lütfen **Ayrıntıları Görüntüle** düğmesine (bu pencerenin alt kısmındadır) basarak ulaşabileceğiniz **Tarama Sonuçları** penceresini inceleyin.

- **Baslangıç zamanı** - taramanın baslatıldığı tarih ve saati gösterir.
- **Bitiş zamanı** - taramanın bittiği tarih ve saati gösterir.
- **Taranan nesneler** - tarama sırasında kontrol edilen nesne sayisidir
- **Bulasmalar** - tespit edilen / silinen [virüs bulasmaları](#) sayısı
- **Casus yazılım** - tespit edilen / silinen [casus yazılım](#) sayısı
- **Uyarılar** - algılanan [süpheli nesnelerin](#)
- **Kök dizinler** - algılanan [kök dizinlerin](#)
- **Tarama kaydı bilgileri** - tarama işlemine ve sonucuna ilişkin bilgiler (genellikle islemin tamamlanmasının ya da kesilmesinin hemen ardından görüntülenir)

Kontrol düğmeleri

Tarama sonuçlarına genel bakış penceresindeki kontrol düğmeleri şunlardır:

- **Ayrıntıları görüntüle** - seçili taramada ayrıntılı verileri görüntülemek için [Tarama sonuçları](#) iletişim kutusuna geçmek için basın
- **Sonucu sil** - seçili öğeyi tarama sonuçlarına genel bakıştan silmek için basın
- **Geri** - [AVG tarama arayüzünün öntanımlı iletişim penceresine geri döner](#)

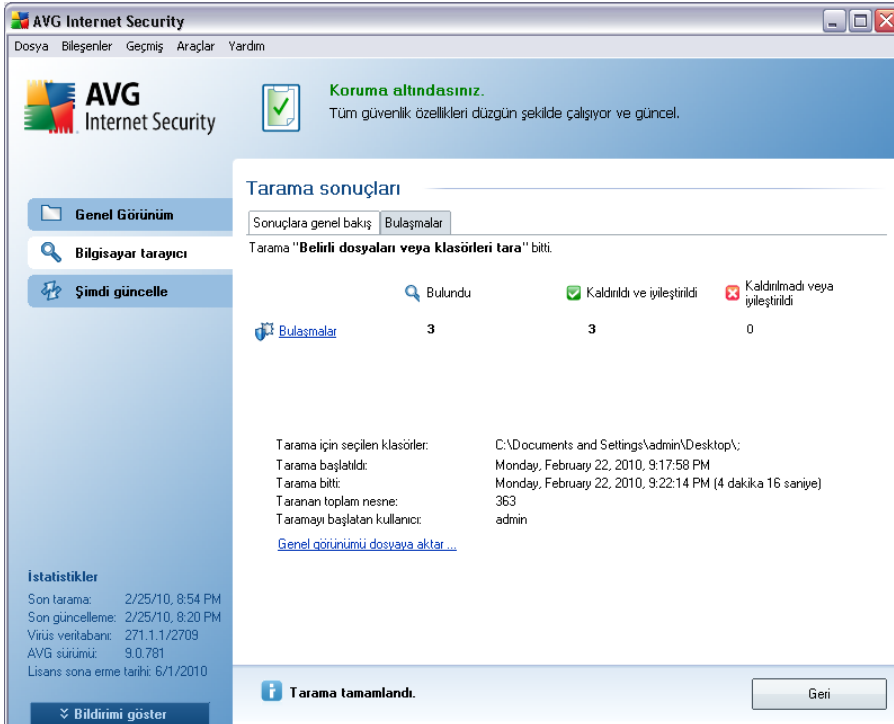
11.7. Tarama Sonuçları Ayrıntılar

[Tarama Sonuçlarına Genel Bakış](#) penceresinde belirli bir tarama türü seçildiyse tarama ve seçilen taramanın sonuçları hakkında ayrıntılı bilgi veren **Tarama Sonuçları** penceresini açmak için **Ayrıntıları görüntüle** düğmesine tıklayabilirsiniz.

İletişim penceresi çok sayıda sekmeye ayrılır:

- **Sonuçlara Genel Bakış** - bu sekme daima görüntülenir ve tarama işlemini tanımayan istatistiki veriler sunar.
- **Bulaşmalar** - bu sekme tarama sırasında virüs bulaşması tespit edilirse görüntülenir
- **Casus yazılım** - bu sekme tarama sırasında casus yazılım tespit edilirse görüntülenir
- **Uyarılar** - bu sekme, örneğin tarama sırasında tanımlama bilgileri algılandığında görüntülenir
- **Bilgi** - bu sekme, yukarıdaki kategorilerde sınıflandırılmayan potansiyel tespit edildiğinde görüntülenir; ardından söz konusu sekmeye buluntu hakkında bir uyarı mesajı görüntülenir. Ayrıca, burada taranamayan nesneler hakkında bilgi de bulacaksınız (örn. parola korumalı arşivler).

11.7.1. Sonuçlara Genel Bakış Sekmesi





Tarama sonuçları sekmesinde aşağıdaki hususlar hakkında ayrıntılı istatistikler ve bilgi bulabilirsiniz:

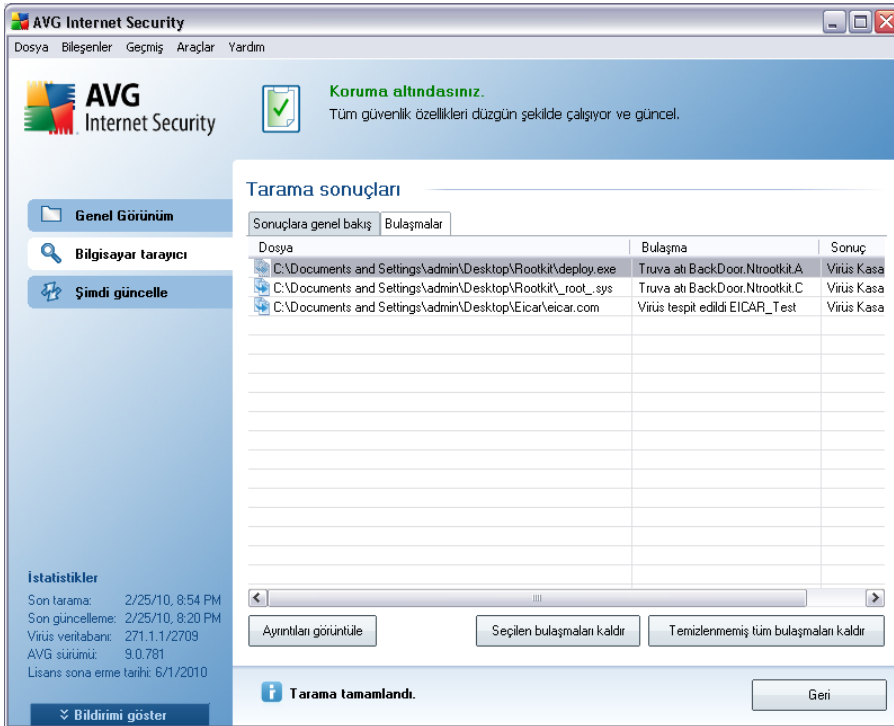
- tespit edilen [virüs bulaşmaları](#) / [casus yazılım](#)
- silinen [virüs bulaşmaları](#) / [casus yazılım](#)
- kaldırılamayan ya da temizlenemeyen [virüs bulaşması](#) / [casus yazılım](#) sayısı

Buna ek olarak, tarama başlangıcı hakkında tarih ve zaman verileri, toplam taranan nesne sayısı, tarama süresi ve tarama sırasında ortaya çıkan hataların sayısı hakkında da bilgi bulabilirsiniz.

Kontrol düğmeleri

Bu iletişim kutusunda sadece bir adet düğme bulunmaktadır. **Sonuçları kapat** düğmesi [Tarama sonuçlarına genel bakış](#) iletişim kutusuna dönmenizi sağlar.

11.7.2. Bulaşma Sekmesi



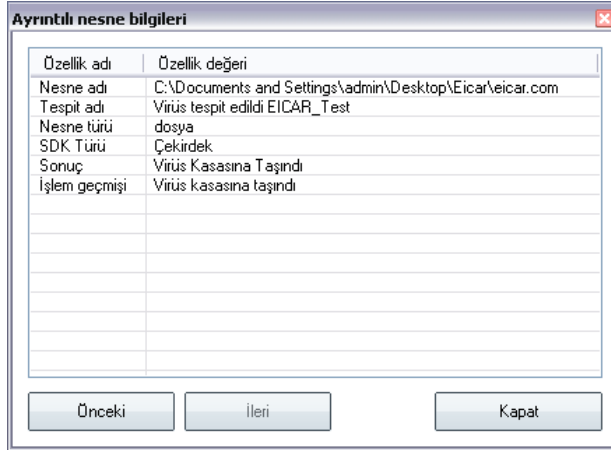
Tarama sırasında bir [virüs bulasmasi](#) tespit edilirse ilgili **Bulasmalar** sekmesi sadece **Tarama Sonuçları** iletişim penceresinde görüntülenir. Sekme, su bilgileri sağlayan üç bölüme ayrılmıştır:

- **Dosya** - bulasmis nesnenin orijinal konumunun tam dizin yolu
- **Bulasmalar** - tespit edilen [virüs](#)ün adı (belirli virüs türleri hakkında ayrıntılı bilgi almak için lütfen çevrimiçi [Virüs Ansiklopedisine](#) danisin)
- **Sonuç** - tarama sırasında tespit edilen bulasmis nesnenin mevcut durumunu tanımlar:
 - o **Bulasanlar** - bulasan nesne tespit edildi ve original konumunda bırakıldı (örneğin _ belirli bir tarama işlemi sırasında otomatik temizleme seçeneğini devre dışı bıraktıysanız)
 - o **Temizlenenler** - bulasmis nesne otomatik olarak temizlenmiştir ve orijinal konumunda bırakılmıştır
 - o **Virüs Kasasına Tasınanlar** - bulasmis nesne [Virüs Kasası](#) karantinasına taşınmıştır
 - o **Silinenler** - bulasmis nesne silinmiştir
 - o **PUP istisnalarına eklenenler** - bulgu bir istisna olarak değerlendirilmiş ve PUP istisnaları listesine eklenmiştir (gelişmiş ayarların [PUP İstisnaları](#) penceresinden yapılandırılır)
 - o **Kilitli dosya - taranamayanlar** - ilgili nesne kilitlidir ve bu nedenle AVG tarafından taranamamaktadır
 - o **Poransiyel olarak tehlikeli nesne** - nesnenin potansiyel anlamda tehlikeli olduğu tespit edilmiş fakat nesneye herhangi bir virüs bulasmamıştır (örneğin makro içeriyor olabilir); bilgi sadece uyarı amaçlıdır
 - o **Eylemi tamamlamak için bilgisayarınızın yeniden başlatılması gerekmektedir** - bulasmis nesne silinememektedir ya da nesneyi tamamen silmek için bilgisayarınızın yeniden başlatılması gerekmektedir

Kontrol düğmeleri

Bu iletişim kutusunda kullanılabilir üç kontrol düğmesi var:

- **Ayrıntıları görüntüle** - düğme **Tarama sonuçları hakkında ayrıntılı bilgi isimli yeni bir pencere açar**:



Bu iletişim kutusunda tespit edilen bulasıcı nesnenin konumuna dair bilgileri bulabilirsiniz(**Nesne adı**). **Geri /İleri** düğmelerini kullanarak belirli bulgular hakkında ayrıntılı bilgi görüntüleyebilirsiniz. Pencereyi kapatmak için **Kapat** düğmesine tıklayın.

- **Seçilen bulasmaları temizle** - seçilen nesneleri [Virüs Kasasına tasımak için düğmeyi kullanın](#)
- **Temizlenmeyen tüm bulasmaları sil** - bu düğme temizlenemeyen ya da [Virüs Kasasına tasınamayan tüm nesneleri siler](#)
- **Sonuçları kapat** - ayrıntılı bilgi penceresini kapatır ve [Tarama sonuçlarına genel bakış](#) penceresine döner

11.7.3. Casus Yazılım Sekmesi

Tarama sırasında bir [casus yazılım](#) tespit edilirse ilgili **Casus Yazılım** sekmesi sadece **Tarama Sonuçları** iletişim penceresinde görüntülenir. Sekme, su bilgileri sağlayan üç bölüme ayrılmıştır:

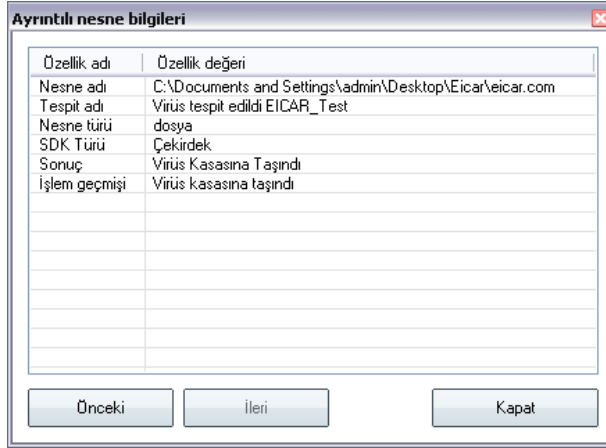
- **Dosya** - bulasmis nesnenin orijinal konumunun tam dizin yolu
- **Bulasmalar** - tespit edilen [casus yazılım](#)ın adı(*belirli virüs türleri hakkında ayrıntılı bilgi almak için lütfen çevrimiçi [Virüs Ansiklopedisine](#) danışın*)
- **Sonuç** - tarama sırasında tespit edilen nesnenin mevcut durumunu tanımlar:

- o **Bulasanlar** - bulasan nesne tespit edildi ve original konumunda bırakıldı (örneğin _ belirli bir tarama işlemi sırasında otomatik temizleme seçeneğini devre dışı bıraktıysanız)
- o **Temizlenenler** - bulaşmış nesne otomatik olarak temizlenmiştir ve orijinal konumunda bırakılmıştır
- o **Virüs Kasasına Tasinanlar** - bulaşmış nesne [Virüs Kasası](#) karantinasına tasınmıştır
- o **Silinenler** - bulaşmış nesne silinmiştir
- o **PUP istisnalarına eklenenler** - bulgu bir istisna olarak değerlendirilmiş ve PUP istisnaları listesine eklenmiştir (*gelişmiş ayarların [PUP İstisnaları](#) penceresinden yapılandırılır*)
- o **Kilitli dosya - taranamayanlar** - ilgili nesne kilitlidir ve bu nedenle AVG tarafından taranamamaktadır
- o **Poransiyel olarak tehlikeli nesne** - nesnenin potansiyel anlamda tehlikeli olduğu tespit edilmiş fakat nesneye herhangi bir virüs bulaşmamıştır (örneğin makro içeriyor olabilir); bilgi sadece uyarı amaçlıdır
- o **Eylemi tamamlamak için bilgisayarınızın yeniden başlatılması gerekmektedir** - bulaşmış nesne silinememektedir ya da nesneyi tamamen silmek için bilgisayarınızın yeniden başlatılması gerekmektedir

Kontrol düğmeleri

Bu iletişim kutusunda kullanılabilir üç kontrol düğmesi var:

- **Ayrıntıları görüntüle** - düğme, **Tarama sonuçları hakkında ayrıntılı bilgi** isimli yeni bir iletişim kutusu penceresi açar:

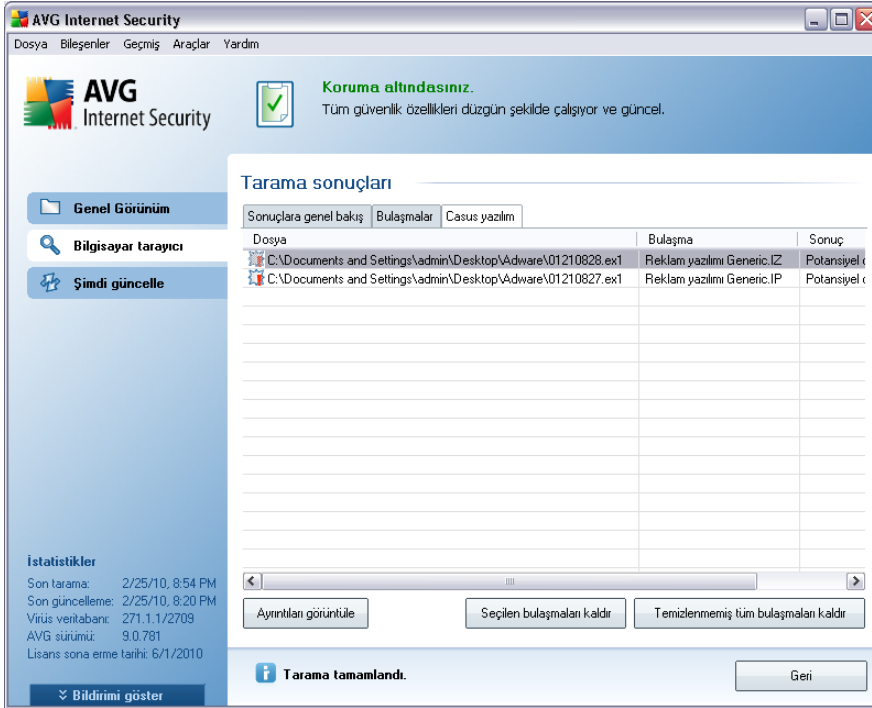


Bu iletişim kutusunda tespit edilen bulasıcı nesnenin konumuna dair bilgileri bulabilirsiniz(**Nesne adı**). **Geri /İleri** düğmelerini kullanarak belirli bulgular hakkında ayrıntılı bilgi görüntüleyebilirsiniz. Pencereyi kapatmak için **Kapat** düğmesine tıklayın.

- **Seçilen bulasmaları temizle** - seçilen nesneleri [Virüs Kasasına tasimak için düğmeyi kullanin](#)
- **Temizlenmeyen tüm bulasmaları sil** - bu düğme temizlenemeyen ya da [Virüs Kasasına tasinamayan tüm nesneleri siler](#)
- **Sonuçları kapat** - ayrıntılı bilgi penceresini kapatır ve [Tarama sonuçlarına genel bakis](#) penceresine döner

11.7.4. Uyarılar Sekmesi

Uyarılar sekmesinde, tarama sırasında tespit edilip "şüpheli duyulan" nesneler (*tipik olarak dosyalar*) hakkında çeşitli bilgiler görüntülenir. [Yerlesik Kalkan](#) tarafından tespit edildiği zaman tespit edilen dosyalara erişim engellenir. Bu şekilde tespit edilen buluntulardan bazıları gizli dosyalar, tanımlama bilgileri, şüpheli kayıt anahtarları, parola korumalı belgeler ya da arşivlerdir. Bu dosyalar bilgisayarınıza ya da güvenliğinize karşı doğrudan tehlike teşkil etmez. Bu dosyalar hakkında verilen bilgiler, bilgisayarınızda reklam yazılımı ya da casus yazılım tespit edildiği durumlarda oldukça yararlıdır. AVG testi tarafından sadece Uyarılar tespit edildiyse herhangi bir işlem yapmanıza gerek kalmaz.



Aşağıda bu tür nesnelere ilişkin en yaygın örnekler kısaca açıklanmıştır:

- **Gizli dosyalar** - Gizli dosyalar, Windows'da varsayılan olarak görülmez durumdadır ve bazı virüsler ya da diğer tehditler dosyalarını söz konusu gizli dosyalara kaydederek algılanma ihtimallerini ortadan kaldırmaya çalışır. AVG'niz, zararlı olabileceğinden şüphelendiğiniz gizli bir dosya rapor ederse, **AVG Virüs Kasası**'na tasiyabilirsiniz.
- **Tanımlama Bilgileri** - Tanımlama bilgileri, kullanıcılara ilişkin bilgileri kaydetmek ve daha sonra söz konusu bilgileri web site şablonlarını yükleme ve kullanıcı adını girmek üzere web siteleri tarafından kullanılan düz metin dosyalarıdır.
- **Şüpheli kayıt anahtarları** - Bazı kötü amaçlı yazılımlar, sistem başlatıldığında yüklendiğinden emin olmak ya da işletim sistemi üzerindeki etkisini artırmak üzere bilgilerini Windows kayıt defterine kaydeder.

11.7.5. Kök Kullanıcı Sekmesi

Rootkit'ler sekmesi, **Rootkit Önleme tarama** başlattıysanız veya manuel olarak kök dizin önleme tarama seçeneğini **Tüm Bilgisayarın Taranması** (bu seçenek varsayılan olarak kapalıdır) içine eklediyseniz tarama sırasında algılanan rootkit'ler hakkında bilgi görüntüler.

Rootkit, sistem yöneticisinin izni olmaksızın yasal olmayan şekillerde bilgisayar sisteminin kontrolünü ele almak için tasarlanmış bir programdır. Kök kullanıcı, donanım üzerinde çalışan işletim sisteminin kontrolünü ele geçirmeyi hedeflediği için donanımsal açıdan erişime gerek duymaz. Genellikle kök kullanıcılar, standart işletim sistemi güvenlik mekanizmalarını dönüştürerek ya da istila ederek sistem üzerindeki varlıklarını gizlerler. Sıklıkla Truva Ati biçimindedirler, dolayısıyla kullanıcıları sistemleri üzerinden çalışacak kadar güvenli olduklarına inandırır. İzleme programlarının çalışan işlemlerini gizlemek ya da işletim sisteminin sistem bilgilerini ya da dosyalarını saklamak, bunu sağlamak için kullanılan teknikler arasında bulunmaktadır.

Bu sekmenin yapısı temel olarak **Bulasmalar sekmesi** ya da **Casus Yazılım sekmesi** ile aynıdır.

11.7.6. Bilgi Sekmesi

Bilgi sekmesinde, bulasma ya da casus yazılım şeklinde sınıflandırılmayan "buluntular" hakkında bilgi bulunmaktadır. Bunlar tehlikeli şekilde etiketlenebilir ancak söz konusu öğeler hususunda dikkatli olmalısınız. AVG taraması, bulasmayan fakat şüpheli olan dosyaları tespit edebilir. Bu dosyalar **Uyarı** veya **Bilgi** olarak rapor edilir.

Önem derecesi **Bilgiler** aşağıdaki nedenlerden birine bağlı olarak rapor edilebilir:

- **Çalışma zamanı paketli** - Dosya, dosyanın taranmasını önleme çabası olarak değerlendirilebilecek yaygın olmayan paketleyicilerinden biri kullanılarak paketlenmiştir. Diğer bir yandan bu tür dosyalar her rapor edildiğinde virüs teskil etmezler.
- **Çalışma zamanı paketi yinelemeli** - Yukarıdakine benzerdir, ancak yaygın yazılımlar arasında nispeten daha az sıklıkta kullanılır. Söz konusu dosyalar şüphelidir ve kaldırılmaları ya da incelenmeleri için bize gönderilmeleri göz önünde bulundurulmalıdır.
- **Parola ile korunan arşiv ya da belge** - Parola ile korunan dosyalar, AVG (ya da genellikle diğer kötü amaçlı yazılımlara karşı koruma programları) tarafından taranamaz.
- **Makro içeren belge** - Rapor edilen belge, zararlı olabilecek makrolar içermektedir.
- **Gizli uzantı** - Gizli uzantılı dosyalar resimler gibi görünebilir, ancak aslında çalıştırılabilir dosyalar olabilir (örn *resim.jpg.exe*). İkinci uzantı, varsayılan olarak Windows'da görünür değildir ve AVG yanlışlıkla açılmalarını engellemek için bu tür dosyaları rapor eder.
- **Uygun olmayan dosya yolu** - Önemli bir sistem dosyası varsayılan yoldan

baska bir yerden çalışıyorsa (örn. winlogon.exe Windows klasöründen baska bir yerde çalışıyorsa) AVG bu durumu rapor eder. Bazi durumlarda virüsler, sistemde fark edilmemek için standart sistem işlemlerinin adını alır.

- **Kilitli dosya** - Rapor edilen dosya kilitli, bu yüzden AVG tarafından taranamıyor. Bu, genellikle bir dosyanın sistem tarafından kullanılmakta olduğu anlamına gelir (örn. takas dosyası).

11.8. Virüs Kasası



Virüs Kasası AVG taramaları sırasında tespit edilen şüpheli/bulasmış nesnelerin yönetilmesi için güvenli bir ortamdır. Tarama sırasında bulasmış bir nesne tespit edildikten sonra AVG, söz konusu bulaşmayı otomatik olarak temizleyemiyorsa şüpheli nesne hakkında ne yapmak istediğiniz sorulur. Önerilen çözüm, nesneyi daha sonra ilgilenmek üzere **Virüs Kasasına** tasimaktır. **Virüs Kasası**'ni satın almanın ana amacı silinen bir dosyayı belirli bir süre için saklamasıdır, böylece dosyayı orijinal konumunda artık istemediğinizden emin olabilirsiniz. Dosyanın yokluğu sorun oluştuyorsa, bu dosyayı analize gönderebilir veya orijinal konumuna geri yükleyebilirsiniz.

Virüs Kasası arayüzü, yeni bir pencerede açılır ve karantina altındaki bulasmış nesneler hakkında genel bilgi içerir:

- **Önem seviyesi** - bulaşma türü hakkında bilgi (*bulaşma seviyesine göre bu kısımda sağlanır - listelenen tüm nesnelere virüs bulaşmıştır veya bulaşma olasılığı vardır*)
- **Virüs Adı** - [Virüs ansiklopedisi](#)'ne (çevrimiçi) göre tespit edilen bulaşmanın adını görüntüler
- **Dosya yolu**- Bulasmış dosyanın orijinal konumuna giden tam yol
- **Orijinal nesne adı** - Tabloda listelenmekte olan tespit edilmiş nesneler, tarama işlemi sırasında AVG tarafından verilen standart isim ile etiketlenmiştir. Nesnenin bilinmeyen farklı bir adı olması halinde (Örn. bir e-posta ekinin adının ekin mevcut içeriğine yanıt vermemesi halinde), söz konusu isim bu sütunda gösterilecektir.
- **Saklama tarihi**: Şüpheli dosyanın tespit edildiği ve Virüs Kasasına kaldırıldığı tarih ve saat

Kontrol düğmeleri

Virüs Kasası arayüzünden ulaşabileceğiniz kontrol düğmeleri şunlardır:

- **Geri Yükle** - bulasmis dosyayı sabit diskinizdeki orijinal konumuna geri yükler
- **Farklı Geri Yükle** - tespit edilen şüpheli nesneyi **Virüs Kasasından** seçilen bir klasöre geri yüklemek için bu düğmeyi kullanın. Şüpheli ve tespit edilen nesne orijinal adıyla kaydedilecektir. Orijinal adı bilinmiyorsa standart adı kullanılacaktır.
- **Ayrıntılar** - bu düğme yalnızca **Identity Protection** tarafından algılanan tehlikeler içindir. Tıklatıldığında, tehlike ayrıntılarının özet genel görünümünü görüntüler (*hangi dosyalar/islemler etkilendi, islemin özellikleri vb.*). IDP'nin algıladığı dışındaki diğer tüm öğeler için, bu düğmenin gri ve devre dışı olduğunu unutmayın!
- **Sil** - bulasmis dosyayı **Virüs Kasasından** tamamen ve geri dönüştürülemez şekilde siler
- **Kasayı Bosalt** - **Virüs Kasası** içeriğini tamamen temizler. Dosyaları Virüs Kasası'ndan kaldırdığınızda, bu dosyalar diskten geri dönüştürülemez şekilde kaldırılır (Geri Dönüşüm Kutusu'na gitmez).

12. AVG Güncellemeleri

Yeni bulunan tüm virüslerin mümkün olduğunca çabuk algılanabilmesi için AVG'nizi güncel tutmak çok önemlidir.

[AVG Yükleme süreci](#) sırasında, AVG'nizi ne sıklıkta güncellemek istediğinizi belirtirsiniz. Kullanılabilir seçenekler **Her 4 saatte bir** veya **Her gün**'dür (bkz. [Düzenli tarama ve güncellemeleri programlama](#) iletişim kutusu). AVG güncellemeleri sabit tarihlerde değil, yeni tehlikelerin miktarına ve önemine göre yayınlandığından, günde en az bir kez yeni güncellemeleri kontrol etmeniz önerilir. Her 4 saatte bir kontrol etme **AVG 9 Anti-Virus** ürününüzün gün boyu güncel kalmasını garantiler.

12.1. Güncelleme Seviyeleri

AVG, arasından seçim yapabileceğiniz iki güncelleme seviyesi sunmaktadır:

- **Tanım güncellemeleri** güvenilir virüsten koruma için gerekli değişiklikleri içerir. Tipik olarak kodu değiştirmemekte, değişiklikler sadece veritabanını kapsamaktadır. Bu güncelleme sunulur sunulmaz yüklenmelidir.
- **Program güncellemeleri** çeşitli program değişikliklerini, onarımlarını ve gelişimlerini içerir.

[Bir güncelleme programlanırken](#) indirme ve uygulanma açısından öncelik sırasını seçmek mümkündür.

Not: Programlanmış bir program güncellemesinin zaman çakışması olursa ve programlanmış tarama gerçekleşirse, güncelleme işlemi yüksek önceliklidir ve tarama kesilir.

12.2. Güncelleme Türleri

İki güncelleme türü arasında seçim yapabilirsiniz:

- **İsteğe Bağlı Güncelleme** ihtiyacınız olduğu durumlarda hemen gerçekleştirilebilecek AVG güncellemesidir.
- **Programlanan güncelleme** - AVG menüsünden [bir güncelleme planı programlayabilirsiniz](#). Planlanan güncelleme, yapılandırma ayarlarınıza bağlı olarak periyodik olarak gerçekleştirilir. Belirli bir konumda yeni güncelleme dosyaları bulunur bulunmaz doğrudan İnternet'te ya da ağ dizininden indirilirler. Yeni güncelleme dosyası yoksa herhangi bir işlem yapılmaz.

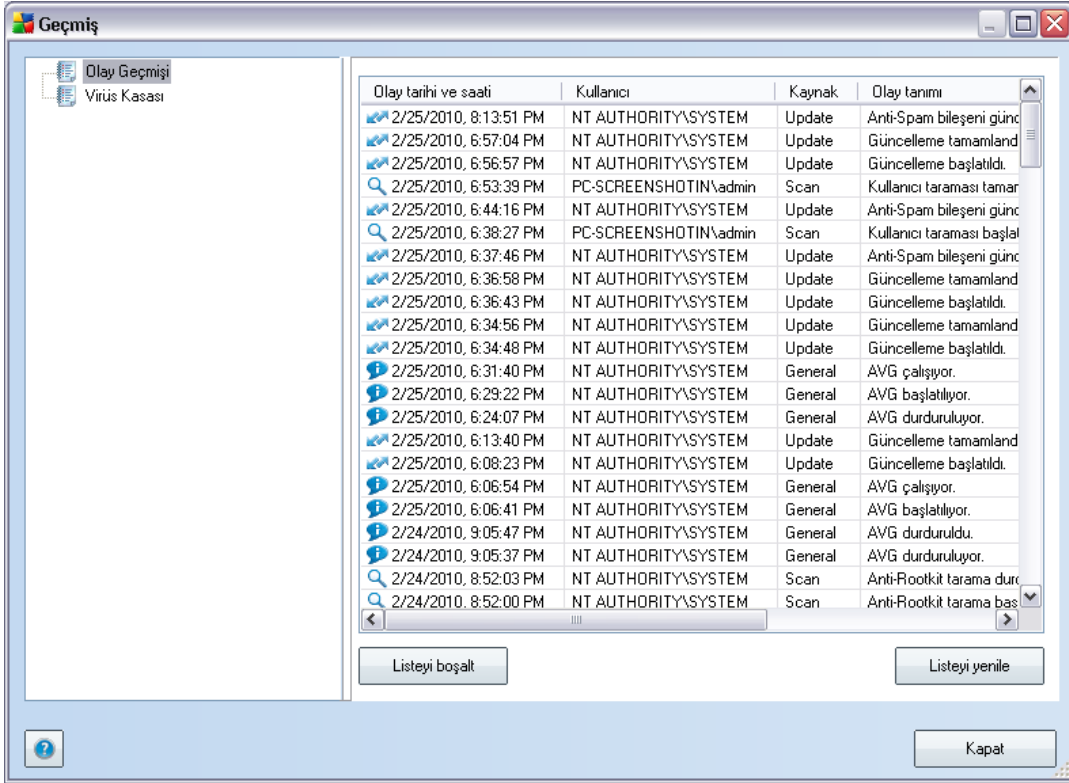
12.3. Güncelleme İşlemi

Güncelleme işlemi **Simdi Güncelle** [hızlı bağlantısına](#) tıklanarak istenilen anda başlatılabilir. Bu bağlantıya bütün [AVG Kullanıcı Arayüzü](#) pencerelerinden ulaşabilirsiniz. Diğer bir yandan [Güncelleme yöneticisi](#) bileşeninden düzenlenebilen güncelleme programlarında planlanan güncellemelerin düzenli olarak yapılması önerilmektedir.

Güncellemeye başladıktan sonra AVG, yeni güncelleme dosyasının olup olmadığını aramaya başlayacaktır. Varsa AVG indirme işlemine başlat ve güncelleme işlemi otomatik olarak başlatır. Güncelleme işlemi sırasında güncelleme işleminin ilerleyişinin yanı sıra ilgili istatistik parametreleri de görüntüleyebileceğiniz **Güncelleme** arayüzüne yeniden yönlendirileceksiniz (*güncelleme dosyasının boyutu, alınan veriler, indirme hızı, kalan süre...*).

Not: AVG program güncellemesi başlatılmadan önce sistem geri yükleme noktası oluşturulur. Güncelleme işleminin başarısız olması ve işletim sisteminizin çökmesi halinde işletme sisteminizi bu noktaya geri döndürebilirsiniz. Bu seçeneğe Baslat/Tüm Programlar bilgisayarınızın günde en az bir kere açıldığından emin olduğunuz durumlarda önerilir/Donatılar /Sistem Araçları /Sistem Geri Yükleme menüsünden erişebilirsiniz fakat değişikliklerin sadece uzman kullanıcılar tarafından yapılması önerilmektedir.

13. Olay Geçmişi



Etkinlik Geçmişi iletişim kutusuna [sistem menüsü](#) üzerinden **Geçmiş/Etkinlik Geçmişi Kayıt Defteri** ögesi vasıtasıyla ulaşabilirsiniz. Bu iletişim kutusu içinde, **AVG 9 Anti-Virus** işlemi sırasında oluşan önemli olayların bir özetini bulabilirsiniz. **Etkinlik Geçmişi** aşağıdaki etkinlik türlerini kaydeder:

- AVG uygulamasının güncellemeleri hakkında bilgi
- Tarama başlangıcı, sonu veya taramanın durdurulması (otomatik olarak gerçekleştirilen taramalar dahil olmak üzere)
- Virüs tespitine ilişkin etkinlikler ve virüsün konumu ([Yerlesik Kalkan](#) ya da [tarama](#) tarafından)
- Diğer önemli etkinlikler

Kontrol düğmeleri



- **Listeyi temizle** - etkinlik listesindeki tüm girisleri siler
- **Listeyi yenile** - etkinlik listesindeki tüm girisleri günceller



14. SSS ve Teknik Destek

İşletmenizde ya da teknik açıdan AVG ile herhangi bir sorun yaşıyorsanız lütfen, AVG web sitesinin (<http://www.avg.com/>) [SSS](#) bölümüne bakın.

Bu şekilde yardım alamazsanız teknik destek bölümüne e-posta ile başvurun. Lütfen **Yardım/Çevrimiçi yardım al** sistem menüsünden ulaşabileceğiniz iletişim formunu kullanın.